2025 FALL CFT NOTE

Ridongen 529900453@qq.com

Contents

1 Preface

This course was taught in Fudan University over the Fall semester of 2025, by Prof. Miaofen Chen.

The content presented herein aims to remain faithful to the structure and flow of the classroom lectures, serving primarily as a companion for review and consolidation of the material.

While every effort has been made to capture the essence of the course, these notes are a product of personal study. Consequently, the reader is kindly asked to bear with any potential omissions of technical details, lack of rigor in certain proofs, or minor inaccuracies that may have occurred during the AI (Using Gemini) transcription process.

The arrangement of the chapters is as follows:

2 2025.9.11

2.1 Introduction

Motivation: splitting problem
Fix $f(x) \in \mathbb{Z}[x]$, monic irreducible.

- **Question A**: Is there a rule which for $\forall p$ prime determines whether $f(x)$ split mod p?

e.g. $f(x) = x^2 + 1$. split iff $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$. In general, such a rule is called **reciprocity law**.

—

History

1. $1700 - 1800+$: quadratic recip. thy.
   - Fermat, Euler, Gauss.

   Solve Question A for f of deg $= 2$.

2. early 1900s: Furtwängler, Hilbert, Artin.
   - Class field theory

   Solve Question A for $f(x)$ with solvable Galois gp.

3. 1960+ : Eichler, Shimura, Deligne, Serre.
   - 2 dim. Galois rep. $\longleftrightarrow$ modular forms, Geometry of modular curves

   Problem: Some (i.e. for deg=5) f with non-solvable Galois gp.

4. 2000+ Scholze.
   - Galois rep. $\longleftrightarrow$ geom. of arith. manifold.

—

Relation to ANT

Let $L = \mathbb{Q}[x]/(f(x))$.

- Then L is a number field.

Then, we know if $f(x) \in \mathbb{Z}[x]$ is monic irreducible, then except for finitely many primes p,

$$f(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod{p}$$

where $\overline{g_i(x)} \in (\mathbb{Z}/p\mathbb{Z})[x]$ monic irreducible distinct.

$$p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad \text{where } \mathfrak{p}_i = (p, g_i(\alpha)).$$

$$[\mathcal{O}_L/\mathfrak{p}_i : \mathbb{F}_p] = \deg g_i.$$

$(p \nmid N_{L/\mathbb{Q}}(f'(x)))$

Recall: p split in $L \iff r = [L : \mathbb{Q}]$ and $e_i = 1, f_i = 1$. Except for finitely many p, $f(x)$ is split mod p for $f(x)$ is split in L.

For L/K extension of number fields. **Question B**: Is there a rule which for each prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ determines whether $\mathfrak{p}$ is split in L?

Equivalently, want to describe

$$\{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \text{ prime} \mid \text{splits in } L\}.$$

This set is denoted as $\operatorname{Spl}(L/K)$.

—-

Exercise: Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal, L/K be a finite extension. Then $\mathfrak{p}$ splits in $L \iff \mathfrak{p}$ splits in L' where L' is the Galois closure of L/K.

Fact: Let K be a number field, $L_1/K, L_2/K$ be finite Galois extensions. If $L_1 \supseteq L_2$, then obviously $\operatorname{Spl}(L_1/K) \subseteq \operatorname{Spl}(L_2/K)$. In fact, If $\operatorname{Spl}(L_1/K) \subseteq \operatorname{Spl}(L_2/K)$, then $L_1 \supseteq L_2$ (This is not obvious, which needs CFT). In particular, $L_1 = L_2 \iff \operatorname{Spl}(L_1/K) = \operatorname{Spl}(L_2/K)$.

Corollary: Fix K. Then $\operatorname{Spl}(L/K)$ can be determined by L for Galois extension L/K. (**Remark:**the Galois assumption is necessary)

e.g.

$$\operatorname{Spl}(\mathbb{Q}(i)/\mathbb{Q}) = \left\{(p) \mid \left(\frac{-1}{p}\right) = 1\right\}$$
$$\operatorname{Spl}(\mathbb{Q}(\sqrt[8]{2})/\mathbb{Q}) = \left\{(p) \mid \left(\frac{2}{p}\right) = 1\right\} = \{p \mid p \equiv 1 \pmod 8\}$$

Suppose L/K is a Galois extension. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Assume $\mathfrak{p}$ is unramified in L/K.

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

for which $\mathfrak{P}_i$ are prime ideals in $\mathcal{O}_L$.

The decomposition group is $D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$.

$$D(\mathfrak{P}_i/\mathfrak{p}) \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}_i/\mathcal{O}_K/\mathfrak{p})$$
$$\left(\frac{L/K}{\mathfrak{P}_\mathfrak{i}}\right) \mapsto \sigma := (x \mapsto x^q) \text{ (isom.)}$$

where $q = |\mathcal{O}_K/\mathfrak{p}|$.

The generator $\left(\frac{L/K}{\mathfrak{P}_\mathfrak{i}}\right)$ is called **Frobenius element**.

—

The conjugacy class doesn't depend on the choice of $\mathfrak{P}_i$.

Suppose L/K is an abelian extension. Then the Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$ doesn't depend on the choice of $\mathfrak{P}_i$.

$$\mathfrak{p} \text{ is split in } L \iff \mathrm{Frob}_\mathfrak{p} = \mathrm{id}.$$

Let $\mathcal{I}_K$ be the group of fractional ideals of $\mathcal{O}_K$. Let $\mathcal{I}_K^L$ be the free abelian group generated by prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in L/K.

The map $\Psi_{L/K} : \mathcal{I}_K^L \to \mathrm{Gal}(L/K)$ is a group homomorphism.

$$\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$$

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_r^{s_r} \mapsto \mathrm{Frob}_{\mathfrak{p}_1}^{s_1} \cdots \mathrm{Frob}_{\mathfrak{p}_r}^{s_r}$$

In fact, the map is surjective. So:

$$\mathrm{Gal}(L/K) \cong \mathcal{I}_K^L/\ker\, \Psi_{L/K}$$

The kernel of the map $\Psi_{L/K}$ provides a way to understand Question B, which needs Class Field Theory.

Recall: Chebotarev density theorem

Fix a conjugacy class $C \subset \mathrm{Gal}(L/K)$. The set of prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified and $\mathrm{Frob}_\mathfrak{p} \in C$ has a density of $\frac{1}{[L:K]}$. The theorem needs CFT to prove.

Example: Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$. The result is called **Dirichlet density theorem**.

—

The **Goal of Class Field Theory** is to describe all the abelian extensions of K. When K is a number field, this is **Global Class Field Theory**. When K is a local field (e.g., p-adic field), this is **Local Class Field Theory**.

(Global field) $K \rightsquigarrow K_v$ (local field)

Let V_K be the set of places of K. The adele ring of K is $\mathbb{A}_K := \prod'_{v \in V_K} K_v$, which is the restricted product.

$$\mathbb{A}_K = \{(x_v)_{v \in V_K} \mid x_v \in \mathcal{O}_{K_v} \text{ for almost all } v \in V_K\}$$

K embeds diagonally into $\mathbb{A}_K$.

The group of ideles of K is $\mathbb{A}_K^\times := \prod'_{v \in V_K} K_v^\times$.

$$\mathbb{A}_K^\times = \{(x_v)_{v \in V_K} \mid x_v \in \mathcal{O}_{K_v}^\times \text{ for almost all } v \in V_K\}$$

$K^\times$ embeds diagonally into $\mathbb{A}_K^\times$.

The idele class group is $C_K := \mathbb{A}_K^\times / K^\times$. It is a topological group.

—

The idele class group map is $\Psi_{L/K} : \mathbb{A}_K^\times \to \mathcal{I}_K : (x_v)_v \mapsto \prod_v \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}$ This is a reasonable group homomorphism. In fact, it is surjective. Moreover it induces a surjective map: $C_K \twoheadrightarrow \mathrm{Cl}_K$.

Example: $K = \mathbb{Q}$. $\mathbb{A}_\mathbb{Q} = \mathbb{R} \times \prod_p \mathbb{Q}_p$. $C_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \simeq \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times$.

Theorem: Suppose L/K is an abelian extension. Then there exists an **Artin reciprocity** map

$$\Psi_{L/K} : C_K \to \mathrm{Gal}(L/K)$$

which is surjective with $\mathrm{Ker}(\Psi_{L/K}) = N_{L/K}(C_L)$.

$$C_K / N_{L/K}(C_L) \simeq \mathrm{Gal}(L/K)$$

In particular, whether a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ splits in L is determined by some congruence condition.

Corollary: When $\mathrm{Gal}(L/K)$ is solvable, we can solve Question B. This generalizes abelian extensions, e.g., for $\mathrm{Gal}(L/K)$ solvable, we can solve for L/K where L is a "tower of abelian extensions."

—

Example $x^4 - 2 \pmod p$ splits $\iff$ p splits in $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{2})$. $\implies$

$$p \equiv 1 \pmod 4 \iff p = \pi\overline{\pi} \text{ where } \pi = a + bi \in \mathbb{Z}[i]$$

In fact, $x^4 - 2 \pmod p$ splits $\iff$ $.p = a^2 + 64c^2, \quad a, c \in \mathbb{Z}$ (This is an example of Class Field Theory).

Example The composite of abelian extensions is still abelian. K^{ab}/K is the union of all finite abelian extensions of K.

$$\mathrm{Gal}(K^{ab}/K) = (\mathrm{Gal}(\overline{K}/K))^{ab}$$

This is the maximal abelian extension of K, also known as the maximal abelian quotient of $\mathrm{Gal}(\overline{K}/K)$.

$$\begin{array}{ccc} C_K & \dashrightarrow & \mathrm{Gal}(K^{ab}/K) \\ \downarrow{\scriptstyle \Psi_{L/K}} & & \downarrow \\ \mathrm{Gal}(L/K) & \xrightarrow{\mathrm{id}} & \mathrm{Gal}(L/K) \end{array}$$

Does $C_K \dashrightarrow \mathrm{Gal}(K^{ab}/K)$ map exist? Yes, denote it as Ψ_K.

Main Theorem of Global Class Field Theory(Takagi-Artin) There is a canonical continuous homomorphism:

$$\Psi_K : C_K \to \mathrm{Gal}(K^{ab}/K)$$

which satisfies the following condition:

(1) (Reciprocity) For any finite abelian extension L/K,

$$C_K \to \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$$

is the Artin map $\Psi_{L/K}$ and is surjective with kernel $N_{L/K}(C_L)$.

(2) (Existence) There is a one-to-one correspondence between finite abelian extensions of K and a certain set of open and finite index subgroups of C_K.

$$L/K \text{ finite abelian extension} \iff \text{open and finite index subgroup of } C_K.$$

where $L \mapsto N_{L/K}(C_L)$.

(3) (Functoriality)

Case when $K = \mathbb{Q}$. Then the **Kronecker-Weber** theorem states that $\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$.

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times$$

Let's check the map from $C_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.

$$\mathbb{R}_{>0}^{\times} \times \prod_p \mathbb{Z}_p^{\times} \to \prod_p \mathbb{Z}_p^{\times}$$

$$(a_\infty, (a_p)_p) \mapsto (a_p)_p$$

Corollary: $L/\mathbb{Q}$ is abelian, then there exists $n \in \mathbb{N}$ such that $L \subseteq \mathbb{Q}(\zeta_n)$ and $\mathrm{Spl}(L/\mathbb{Q}) = \{p \mid \overline{p} \in H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L) \subseteq (\mathbb{Z}/n\mathbb{Z})^*\}$.

Main Result of Local Class Field Theory For a local field K, there is a canonical homomorphism $\Psi_{L/K} : K^{\times} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, which is surjective. It has the same condition as G.C.F.T. The map is a group cohomology over L.C.F.T.

2.2 Review of profinite groups

A directed set $(I, \leq)$ is a set I with a transitive relation $\leq$ such that for all $i, j \in I$, there exists $k \in I$ where $i \leq k$ and $j \leq k$.

An inverse system of sets (or maps, groups, topological spaces) indexed by $(I, \leq)$ is a set $\{X_i\}_{i \in I}$ and for all $i, j \in I$ with $i \leq j$, there is a transitive map $p_{ji} : X_j \to X_i$.

$$p_{ik} : X_k \to X_i \quad \text{if } i \leq j \leq k \quad p_{ji} \circ p_{kj} = p_{ki}$$

For an inverse system of sets $\{X_i\}_{i \in I}$, the inverse limit is defined as $\varprojlim X_i = \{x \in \prod_{i \in I} X_i \mid p_{ji}(x_j) = x_i \text{ for all } i \leq j\}$. Here $p_i : \prod_{i \in I} X_i \to X_i$ is the projection of the i-th coordinate.

For $\{X_i\}_{i \in I}$ an inverse system of topological spaces, the inverse limit $X = \varprojlim X_i$ is given the subspace topology from the product topology of $\prod_{i \in I} X_i$.

Similarly, if $\{X_i\}_{i \in I}$ is an inverse system of topological groups, then so is $\varprojlim X_i$.

3 2025.9.18

I. Adeles and Ideles

3.1 Review of profinite groups

Definition 3.1. A topological group is **totally disconnected** if each connected component has only one point (not necessarily discrete).

Definition 3.2. A topological space is **profinite** if it's Hausdorff, compact, and totally disconnected.

Fact: A topological space is profinite if and only if it is homeomorphic to the inverse limit $\varprojlim X_i$ of an inverse system $(X_i)_{i\in I}$ where the topological spaces X_i are finite sets with the discrete topology.

Definition 3.3. A **topological group** is a group G with a topology such that the multiplication map $G \times G \to G : (x, y) \mapsto xy$ and the inverse map $G \to G : x \mapsto x^{-1}$ are both continuous.

Definition 3.4. A topological group is called **profinite** if its underlying topological space is profinite.

Exercise 3.1. A topological group G is profinite if and only if G is topologically isomorphic to the inverse limit $\varprojlim G_i$ of an inverse system of finite groups with the discrete topology.

Example 3.1.

$$\begin{aligned}
\mathbb{Z}_p &= \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\
\mathrm{Gal}(\overline{K}/K) &= \varprojlim \mathrm{Gal}(L/K) \quad (\text{where } \leftarrow \text{ means } L/K \text{ finite Galois extension}) \\
\mathcal{O}_K &= \varprojlim \mathcal{O}_K/\mathfrak{m}^n \quad (\text{where } K \text{ is a } p\text{-adic field}) \\
\mathcal{O}_K^\times &= \varprojlim \mathcal{O}_K^\times/(1+\mathfrak{m}^n)
\end{aligned}$$

Definition 3.5. Let G be a topological group. The **profinite completion** of G is defined as $\widehat{G} = \varprojlim G/H$, where H is an open normal subgroup of finite index.

We have a natural map $G \to \widehat{G}$, which is a continuous group homomorphism of topological groups.

Example 3.2. Let $(\mathbb{Z}, +)$ be a group with the discrete topology. Then its profinite completion is:

$$\begin{aligned}\widehat{\mathbb{Z}} &= \varprojlim \mathbb{Z}/n\mathbb{Z} \\ &\simeq \prod_p \mathbb{Z}_p\end{aligned}$$

3.2 Restricted product

Definition 3.6. Let V be a set and $(X_v)_{v\in V}$ be a family of topological spaces. For almost all $v \in V$, we fix an open set $U_v \subset X_v$. The **restricted product** of $(X_v)_{v\in V}$ with respect to $(U_v)_{v\in V}$ is defined as:

$$X = \prod_{v\in V}{}' X_v = \{(x_v)_{v\in V} \mid x_v \in U_v \text{ for almost all } v\}$$

It is equipped with the topology generated by basic open sets of the form $\prod_{v\in S} Y_v \times \prod_{v\in S^c} U_v$, where $S \subset V$ is a finite set containing all $v \in V$ such that U_v is not defined, and $Y_v \subset X_v$ is an open subset for all $v \in S$.

Remark: If we change choice of U_v for finitely many v, then X and its topology does NOT change.

1. If $U_v = X_v$ for almost all v, then $X = \prod_{v\in V} X_v$ and its topology is the product topology.

Proposition 3.1. If each X_v are locally compact (any pt. has compact nbhd.), Hausdorff and U_v are all compact, then $X = \prod'_{v\in V} X_v$ is locally compact, Hausdorff.

Lemma 3.1. Let $S \subset V$ be a finite set of indices containing all v's s.t. U_v is not defined. Then $X_S := \prod_{v\in S} X_v \times \prod_{v\in S^c} U_v \subset X$ is open, and **the subspace topo. on $X_S \subset X$ coincides with product topo. on X_S**

Proof. of proposition:

Claim: $\forall S \in V$ as in Lemma, X_S is locally cpt. and Hausdorff.

Consider product topo. of X_S:

- (Arbitrary many cpt. set, their product is still compact) $\implies$ X_S is locally cpt.
- easily $\implies$ X_S is Hausdorff.

$X = \bigcup_S X_S$. X is locally cpt. (locally cpt. is a local condition).

$\forall x \in X, \exists S_1, S_2$ s.t. $x \in X_{S_1}, y \in X_{S_2}$. Obviously $X_{S_1}, X_{S_2} \in X_{S_1 \cup S_2}$. $\implies$ consider $x, y \in X_{S_1 \cup S_2}$ $\implies$ X is Hausdorff. □

3.3 Adeles

Let K be a number field. Let V_K be the set of places of K.

$$V_{K,\infty} := \text{set of infinite places of } K$$
$$V_{K,f} := \text{set of finite places of } K$$
$$V_K = V_{K,\infty} \amalg V_{K,f}$$

Definition 3.7. The **ring of adeles** $\mathbb{A}_K$ is the restricted product of $(K_v)_{v \in V_K}$ with respect to $(\mathcal{O}_v)_{v \in V_{K,f}}$.

$$\mathbb{A}_K = \prod_{v \in V_K}{}' K_v$$

Addition on $\mathbb{A}_K$: $(x_v)_{v \in V_K} + (y_v)_{v \in V_K} = (x_v + y_v)_{v \in V_K}$. Multiplication on $\mathbb{A}_K$: $(x_v)_{v \in V_K} \cdot (y_v)_{v \in V_K} = (x_v y_v)_{v \in V_K}$.

Remark:

1. $\mathbb{A}_K$ is a locally compact, Hausdorff topological ring.
2. There is a natural map $K \to \mathbb{A}_K$, $x \mapsto (x)_v$.

It is a ring homomorphism.

Example 3.3. $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \prod_p' \mathbb{Q}_p = \mathbb{R} \times (\prod_p \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q}) = \mathbb{R} \times (\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q})$

Exercise 3.2. Let L/K be an extension of number fields. The natural map $L \otimes_K \mathbb{A}_K \to \mathbb{A}_L$ is an isomorphism of topological rings. Here we equip product topology of $L \otimes_K \mathbb{A}_K$

after choosing a basis of L/K. The map $L \otimes_K \mathbb{A}_K \to \mathbb{A}_L$ comes from:

$$K_v \otimes_K L \to \prod_{w|v \in V_L} L_w \text{ diagonal embedding}$$

And in fact: $L \otimes_K \mathbb{A}_K \cong \mathbb{A}_L$ "$\cong$" does NOT depend on choice of basis.

Theorem 3.1. The image of the natural map $K \to \mathbb{A}_K$ is discrete. The quotient topology on $\mathbb{A}_K/K$ is compact.

Step 1: Reduce to the case $K = \mathbb{Q}$.

- Apply Ex. to $K/\mathbb{Q}$, choose a basis of K over $\mathbb{Q}$. $\mathbb{A}_K \cong K \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}} \cong \mathbb{Q}^n \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}} \cong (\mathbb{A}_{\mathbb{Q}})^n$ where $K \subseteq \mathbb{A}_K$ corresponds to $\mathbb{Q}^n \subseteq (\mathbb{A}_{\mathbb{Q}})^n$. Then $\mathbb{A}_K/K \cong (\mathbb{A}_{\mathbb{Q}}/\mathbb{Q})^n$

Therefore, it suffices to prove the theorem for $K = \mathbb{Q}$.

Step 2: prove the case $K = \mathbb{Q}$.

- $\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q}}$ is discrete.

It suffices to show there exists an open neighbourhood of 0, say $U \subset \mathbb{A}_{\mathbb{Q}}$, s.t. $U \cap \mathbb{Q} = \{0\}$. Let $U = (-1, 1) \times \prod_p \mathbb{Z}_p \subset \mathbb{A}_{\mathbb{Q}}$ be an open set. $\forall x \in \mathbb{Q} \cap U$, $x \in (-1, 1)$ and $x \in \mathbb{Z}_p$ for all primes p. $x \in \mathbb{Z}_p$ for all prime $p \implies x \in \mathbb{Z}$. So we have $x \in \mathbb{Z}$ and $-1 < x < 1$, which implies $x = 0$.

- $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact.

It suffices to show there exists a compact subset $C \subset \mathbb{A}_{\mathbb{Q}}$ s.t. the natural map $\mathbb{A}_{\mathbb{Q}} \to \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is surjective. (Because for continuous map compact set can be sent to compact set.) $C = [0, 1] \times \prod_p \mathbb{Z}_p$. C is compact. Let $x = (x_v) \in \mathbb{A}_{\mathbb{Q}}$. $\forall v = p$, s.t. $x_p \notin \mathbb{Z}_p$, $x_p = a_p + b_p$ where $a_p \in \{1, \ldots, p^k - 1\} \cdot \frac{1}{p^k}$, $b_p \in \mathbb{Z}_p$.

$S = \{v = p \mid x_p \notin \mathbb{Z}_p\}$ finite subset. $a_p \in \mathbb{Z}_l$ for $l \neq p$ prime, Let $a_\infty \in \mathbb{Z}$ s.t. $x_\infty - a_\infty - \sum_{p \in S} a_p \in [0, 1]$.

Hence let $y = \sum_{p \in S} a_p + a_\infty \in \mathbb{Q}$. $(x_v - y_v) \in C$. Use the image of compact is still compact.

3.4 Ideles

Definition 3.8. The **group of ideles** $\mathbb{I}_K := \prod'_{v\in V_K} K_v^\times$ is the restricted product with respect to $\mathcal{O}_{K_v}^\times \subseteq K_v^\times$ for almost all $v \in V_K$.

Remark:

1. $\mathbb{I}_K$ is a locally compact, Hausdorff topological group.
2. As a group, $\mathbb{I}_K = \mathbb{A}_K^\times$. But the topology of $\mathbb{I}_K$ is finer than the subspace topology of $\mathbb{A}_K$.

Exercise 3.3.
1. $\mathbb{I}_K \hookrightarrow \mathbb{A}_K$ is continuous but not a homeomorphism onto the image.
2. $\mathbb{I}_K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K : x \mapsto (x, x^{-1})$ is a homeomorphism onto the image.

Definition 3.9. The **idele norm** is a homomorphism $|\cdot| : \mathbb{I}_K \to \mathbb{R}_{>0}$.

$$(x_v) \mapsto \|x\| = \prod_{v\in V_K} \|x_v\|_v$$

where $\|\cdot\|_v$ is the normalized absolute value at v.

Recall: The normalized absolute value $\|x_v\|_v$ is defined as:

$$\begin{aligned} \|x_v\|_v &= |\mathcal{O}_v/(\pi_v)|^{-ord_p(x_v)} && v = p \\ \|x_v\|_v &= |x_v| && K_v = \mathbb{R} \\ \|x_v\|_v &= |x_v|^2 && K_v = \mathbb{C} \end{aligned}$$

$\forall x \in K^\times$, $\prod_{v\in V_K} \|x_v\|_v = 1$ (product formula).

Definition 3.10. The **unit ideles** is $\mathbb{I}_K^1 := (\mathbb{A}_K^\times)^1 := \ker(\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0})$.

Remark: $K^\times \subset \mathbb{I}_K^1$ because of the product formula.

Example 3.4. For $K = \mathbb{Q}$, $\|\cdot\| : \mathbb{I}_\mathbb{Q} \to \mathbb{R}_{>0}$ has a section. $\mathbb{R}_{>0} \to \mathbb{I}_\mathbb{Q}$ $r \mapsto (r, 1, 1, \dots)$ Hence, $\mathbb{I}_\mathbb{Q} \cong \mathbb{R}_{>0} \times \mathbb{I}_\mathbb{Q}^1$.

In fact, the map:

$$\prod_p \mathbb{Z}_p^\times \hookrightarrow \mathbb{I}_\mathbb{Q}^1 \twoheadrightarrow \mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$$

is surjective.(the proof is not trivial) Then we will get $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q} \simeq \prod_p \mathbb{Z}_p^\times$ compact.

Remark: The idele norm $\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}$ can be extended to $\mathbb{A}_K$.

$$\begin{array}{ccc} \mathbb{I}_K & \hookrightarrow & \mathbb{A}_K \\ & & \downarrow \\ & & \mathbb{R}_{\geq 0} \\ x = (x_v)_v & \mapsto & \prod_v \|x_v\|_v \end{array}$$

Well-defined. Indeed, if there exists infinitely many $v \in V_K$ s.t. $x_v \in \mathcal{O}_{K_v} \setminus \mathcal{O}_{K_v}^\times$, then $\|x\|_v = 0$.

3.5 Haar measure

Let G be a locally compact, Hausdorff topological group. A **left Haar measure** on G is a non-zero Radon measure μ on G such that $\mu(aU) = \mu(U)$ for all $a \in G$ and any measurable subset $U \subseteq G$.

Fact (Haar): There exists a left Haar measure on G. And any two left Haar measures differ by multiplication by a constant $c \in \mathbb{R}_{>0}$. Similar for right Haar measure.

Example 3.5. $G = (\mathbb{R}, +)$ or $(\mathbb{C}, +)$. Lebesgue measure is a Haar measure.

Remark: If G is abelian then there's no difference between left and right Haar measure. Then we simply say Haar measure.

Lemma 3.2. Let F be a local field. Fix a Haar measure μ_F on $(F, +)$, $\forall x \in F^\times$, $\mu(x \cdot -) = c(x)\mu_F(-)$ for some $c(x) \in \mathbb{R}_{>0}$. $c(x) = \|x\|_F$ for some normalized absolute value $\|\cdot\|_F$ on F.

Proof. 1. If $F = \mathbb{R}$ or $\mathbb{C}$.

Let $B = B(0, 1)$ unit disk. Let μ be the Lebesgue measure.

$$\mu(B) = \begin{cases} 2 & F = \mathbb{R} \\ \pi & F = \mathbb{C} \end{cases}$$

$$\mu(xB) = \begin{cases} |x| \cdot 2 & F = \mathbb{R} \\ \pi|x|^2 & F = \mathbb{C} \end{cases}$$

$\implies c(x) = \|x\|$.

2. F is p-adic.

$\forall x, y \in F^\times, \mu(xy \cdot -) = c(xy)\mu(-) = c(x)\mu(y \cdot -) = c(x)c(y)\mu(-)$. $\implies c : F^\times \to \mathbb{R}_{>0}$ is a group homomorphism. $\|\cdot\| : F^\times \to \mathbb{R}_{>0}$ is also. In order to show $c = \|\cdot\|$, it suffices to show $\forall x \in O_F^\times, c(x) = \|x\|$. Take $x = \pi$ a uniformizer, $c(\pi) = \|\pi\|$.

Take $B = \mathcal{O}_F$. $\forall x \in \mathcal{O}_F^\times, \mu(xB) = \mu(B) \implies c(x) = 1 = \|x\|$. $x = \pi$. $\mu(\pi\mathcal{O}_F) \cdot [\mathcal{O}_F : \pi\mathcal{O}_F] = \mu(\mathcal{O}_F)$ where $q = |\mathcal{O}_F/\pi\mathcal{O}_F|$. (because $\mathcal{O}_F = \bigsqcup_*(* + \pi\mathcal{O}_F)$) $\implies c(\pi) = \frac{1}{q} = \|\pi\|$. □

Corollary 3.1. Let μ be a Haar measure on $(F, +)$. Then a Haar measure $\mu^\times$ on $(F^\times, \cdot)$ is given by:

$$\mu^\times(B) = \int_B \|x\|^{-1} d\mu(x)$$

Let K be a number field. $\forall v \in V_K$ fix a Haar measure μ_v on K_v s.t. $\mu_v(\mathcal{O}_{K_v}) = 1$ for all $v \in V_{K,f}$. Fix a Haar measure $\mu_v^\times$ on $K_v^\times$ s.t. $\mu_v^\times(\mathcal{O}_{K_v}^\times) = 1$. $\forall v \in V_{K,f}$.

Remark: This Haar measure $\mu^\times$ differs from the one in Corollary by a constant.

Fact:

1. There is a unique Haar measure μ on $(\mathbb{A}_K, +)$ satisfying the following condition: For any finite set $S \subseteq V_K$ containing $V_{K,\infty}$ and for any finite family of compact sets $(C_v \subseteq K_v)_{v \in S}$, we have

$$\mu\left(\prod_{v \in S} C_v \times \prod_{v \notin S} \mathcal{O}_{K_v}\right) = \prod_{v \in S} \mu_v(C_v) \times \prod_{v \notin S} \mu_v(\mathcal{O}_{K_v})$$

2. There is a unique Haar measure $\mu^\times$ on $(\mathbb{I}_K, \cdot)$ satisfying the following condition: For any finite set $S \subseteq V_K$ containing $V_{K,\infty}$ and for any finite family of compact sets $(C_v \subseteq K_v^\times)_{v \in S}$, we have

$$\mu^\times\left(\prod_{v \in S} C_v \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times\right) = \prod_{v \in S} \mu_v^\times(C_v) \times \prod_{v \notin S} \mu_v^\times(\mathcal{O}_{K_v}^\times)$$

3.6 Homework

Homework 3.1. Show that there is a canonical isomorphism of topological groups $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, where the product is over all prime number p.

Proof. We prove by constructing morphisms in two directions in the category TopGrp (Hausdorff Topological group).

1. $\hat{\mathbb{Z}} \xrightarrow{\rho} \prod_p \mathbb{Z}_p$

   The map $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ induces $\hat{\mathbb{Z}} \to \mathbb{Z}_p$, which in turn induces the map $\hat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_p \\ \downarrow & & \\ \mathbb{Z}/p^n\mathbb{Z} & & \end{array}$$

2. $\prod_p \mathbb{Z}_p \xrightarrow{\psi} \hat{\mathbb{Z}}$

   Assume $n = p_1^{a_1} \cdots p_k^{a_k}$. By the Chinese Remainder Theorem, we obtain an isomorphism of discrete top groups:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$$

   The map $\prod_p \mathbb{Z}_p \to \mathbb{Z}/n\mathbb{Z}$ is induced by:

$$\begin{array}{ccccc} \prod_p \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & & \\ \downarrow & & \downarrow & \searrow & \\ \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p_1^{a_1}\mathbb{Z} & & \mathbb{Z}/p_i^{a_i}\mathbb{Z} \end{array}$$

   Thus, if $m|n$, we have the commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z} & \longrightarrow & \mathbb{Z}/p_1^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{b_k}\mathbb{Z} \\ \uparrow & & \uparrow \\ \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \end{array}$$

This gives a map $\prod_p \mathbb{Z}_p \to \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$.

$$\begin{array}{ccc} \prod_p \mathbb{Z}_p & \longrightarrow & \varprojlim \mathbb{Z}/n\mathbb{Z} \\ & & \downarrow \\ & & \mathbb{Z}/n\mathbb{Z} \end{array}$$

which induces $\prod_p \mathbb{Z}_p \xrightarrow{\psi} \hat{\mathbb{Z}}$.

Since

$$\begin{array}{ccc} \prod_p \mathbb{Z}_p & \xrightarrow{\rho\psi} & \prod_p \mathbb{Z}_p \\ & \searrow \quad \swarrow & \\ & \mathbb{Z}_p & \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \hat{\mathbb{Z}} & \xrightarrow{\psi\rho} & \hat{\mathbb{Z}} \\ & \searrow \quad \swarrow & \\ & \mathbb{Z}/n\mathbb{Z} & \end{array}$$

By universal property, we have $\rho\psi = \mathrm{id}_{\prod_p \mathbb{Z}_p}$ and $\psi\rho = \mathrm{id}_{\hat{\mathbb{Z}}}$. □

Homework 3.2. Show that a topological group is profinite if and only if it is of the form $\varprojlim_{i\in I} G_i$ for an inverse system $(G_i)_{i\in I}$ of finite groups with discrete topology. Moreover, show that for a profinite group, the open normal subgroups form a neighborhood basis of e.

Lemma 3.3. For a compact Hausdorff space X, the connected component of a point $x \in X$ is given by $C_x = \bigcap_{D\ni x, D \text{ clopen}} D$.

Proof. Let $I_x = \bigcap_{D\ni x, D \text{ clopen}} D$.

- Show $C_x \subseteq I_x$. Since $D \ni x$ is clopen, $D \cap C_x \neq \emptyset$. Since C_x is connected, $D \cap C_x = C_x$, so $C_x \subseteq D$. This holds for all such D, so $C_x \subseteq I_x$.
- Show I_x is connected. Conversely, I_x is an intersection of closed sets, thus compact. If I_x is disconnected, $I_x = A \cup B$ where A, B are disjoint, non-empty, closed (and thus compact) subsets. Since X is compact Hausdorff (thus normal, T_4), there exist disjoint open sets $U, V \subseteq X$ such that $A \subseteq U$ and $B \subseteq V$.

  Since $I_x = \bigcap_\alpha D_\alpha$, where $\{D_\alpha\}$ is the family of all clopen sets containing x. Then $\bigcap_\alpha (D_\alpha \cap (X \setminus (U \cup V))) = I_x \cap (X \setminus (U \cup V)) = \emptyset$.

This is an intersection of compact sets with an empty intersection. Thus, there is a finite sub-intersection that is empty:

$$(D_1 \cap \cdots \cap D_n) \cap (X \setminus (U \cup V)) = \emptyset$$

Let $F = D_1 \cap \cdots \cap D_n$. F is clopen and $F \subseteq U \cup V$.

Then $F \cap U$ and $F \cap V$ are disjoint open sets in F whose union is F. Since F is clopen, $F \cap U$ and $F \cap V$ are clopen in X.

Assume $x \in A \subseteq F \cap U$. Then $F \cap U$ is a clopen set containing x. By definition of I_x, $I_x \subseteq F \cap U$. But $I_x \cap (F \cap V) = B \neq \emptyset$, a contradiction.

Thus I_x is connected. It follows that $I_x = C_x$.

□

Proof of Exercise. Denote $A \equiv$ "G is Compact and totally disconnected."

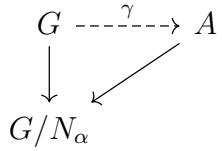
Denote $B \equiv$ "G is a limit of finite discrete top groups."

[A $\implies$ B]

Assume $\{N_\alpha\}_{\alpha \in I}$ is the set of all open normal subgroups of G. Since G is compact, the index $(G : N_\alpha)$ is finite for all α.

Consider the inverse limit $A = \varprojlim_\alpha G/N_\alpha$. The group G/N_α is finite and discrete.

We claim there is a canonical isomorphism $\gamma : G \to A$. The map γ is obtained by the universal property of the inverse limit from the canonical projections $G \to G/N_\alpha$.



Since G is compact and A is Hausdorff, it suffices to show that γ is a bijection.

1. **Injection**: It suffices to show $\bigcap_\alpha N_\alpha = \{e\}$.

   By the first Lemma and the totally disconnectedness of G, for any $x \in G$, $\{x\} = C_x = \bigcap_{D \ni x, D \text{ clopen}} D$.

   So for any $x \neq e$, there exists a clopen set D with $e \in D$ and $x \notin D$.

> **Lemma 3.4.** Let G be a top group, $C \subseteq G$ compact, $A \supseteq C$ open. Then there exists an open neighborhood V of e such that $VC \subseteq A$.

Proof. For each $c \in C$, since multiplication $m : G \times G \to G$ is continuous, there exist open neighborhoods V_c, U_c of e, c respectively such that $V_c U_c \subseteq A$. The sets $\{U_c\}_{c\in C}$ form an open cover of C. Since C is compact, there is a finite subcover $U_{c_1}, \ldots, U_{c_n}$. Let $V = \bigcap_{i=1}^{n} V_{c_i}$. Then V is an open neighborhood of e and $VC \subseteq \bigcup_i VU_{c_i} \subseteq \bigcup_i V_{c_i}U_{c_i} \subseteq A$. □

We use the second Lemma by setting $C = D$ (closed subset of a compact Hausdorff space is compact), $A = D$. Then there exists an open neighborhood V of e such that $VD \subseteq D$.

In particular, because $e \in D$, we have:

$$V \subseteq D$$

Let $W = V \cap V^{-1}$. Then W is a symmetric open neighborhood of e. Consider:

$$H := \bigcup_{n\in\mathbb{Z}} W^n$$

It is a open subgroup of G satisfying:

$$H \subseteq D$$

This is because for all $n \in \mathbb{Z} \setminus \{0\}$, $W^n = W^{|n|} \subseteq V^{|n|-1}D \subseteq D$.

Because G is compact, we have $[G : H] < \infty$ (it not, will contradict with "finite covering" of G). So there are finitely many subgroups of form xHx^{-1}. Consider:

$$N := \bigcap_{x\in G} xHx^{-1}$$

It is an open normal subgroup of G.

We have:

$$N \subseteq H \subseteq D \subseteq G \setminus \{x\}$$

Which means for any $x \neq e$, we can find an open normal subgroup N not containing x. Thus $\bigcap N_\alpha = \{e\}$. γ is injective.

2. **Surjection**: It suffices to show $\gamma(G)$ is dense in A.

   Let $x = (x_\alpha) \in A = \varprojlim G/N_\alpha$. A base of neighborhoods of x is given by sets of the form $\pi_J^{-1}(\{x_\alpha\}_{\alpha\in J})$ for finite $J \subseteq I$.

We want to prove $(\pi_J^{-1}(x_J)) \cap \gamma(G) \neq \emptyset$.

This means we need to find $g \in G$ such that $gN_\alpha = x_\alpha$ for all $\alpha \in J$.

Let $N = \bigcap_{\alpha \in J} N_\alpha$. N is an open normal subgroup.

The condition $gN_\alpha = x_\alpha$ for $\alpha \in J$ is equivalent to finding $g \in G$ such that $gN = x_N$ where x_N is the image of (x_α) in G/N.

The coset x_N is non-empty, so we can pick any element g from it.

Thus $\gamma(G)$ is dense in A. Since $\gamma(G)$ is the continuous image of a compact set, it is compact, hence closed in A.

So $\gamma(G) = A$, and γ is surjective.

So $G \cong \varprojlim G/N_\alpha$ is profinite.

[**B** $\implies$ **A**]
Now assume $G = \varprojlim G_\alpha$, where each G_α is a finite discrete group.

- G_α is compact $\implies \prod G_\alpha$ is compact (Tychonoff). G is a closed subset of $\prod G_\alpha$, so G is compact.
- G_α is Hausdorff $\implies \prod G_\alpha$ is Hausdorff $\implies G$ is Hausdorff.

It remains to show G is totally disconnected. This means the connected component of any point is the point itself. By Lemma 1, for any $x \in G$, $C_x = \{x\}$.

Consider the basis of open sets for the product topology on $\prod G_\alpha$. A basis element is of the form $U = \prod_{\alpha \in S} U_\alpha \times \prod_{\alpha \notin S} G_\alpha$ for a finite set $S \subseteq I$ and $U_\alpha \subseteq G_\alpha$.

Since G_α is discrete, we can take U_α to be singletons. These basis sets are closed (since their complements are also open), so they are clopen.

The topology of G has a basis of clopen sets. For any $x \neq y$, there is a clopen set U containing x but not y.

Then $C_x = \bigcap_{D \ni x, D \text{ clopen}} D \subseteq U$. This implies $y \notin C_x$. Since this holds for all $y \neq x$, $C_x = \{x\}$.

Thus G is totally disconnected. □

Homework 3.3. Let L/K be an extension of number fields. Then we have a diagonal embedding $K_v \to \prod_{w|v} L_w$ for any $v \in V_K$ and hence an embedding $\mathbb{A}_K \to \mathbb{A}_L$.

(a) Show that $\mathbb{A}_K \to \mathbb{A}_L$ is a homeomorphism onto a closed subring of $\mathbb{A}_L$.

(b) We equip the product topology on $L \otimes_K \mathbb{A}_K$ after choosing a K-basis of L (i.e. $L \otimes_K \mathbb{A}_K \cong \mathbb{A}_K^{[L:K]}$). Show that this topology doesn't depend on the choice of the

basis.

(c) Show that the natural map $L \otimes_K \mathbb{A}_K \to \mathbb{A}_L$ is an isomorphism of topological rings.

Proof. (a) Let $\phi : \mathbb{A}_K \to \mathbb{A}_L$ be the embedding. Consider $\psi : \phi(\mathbb{A}_K) \to \mathbb{A}_K$ which is the projection $(y_w)_w \mapsto (x_v)_v$ where $x_v = y_w$ for any $w|v$. Then $\phi\psi = \mathrm{id}$ and $\psi\phi = \mathrm{id}$. ϕ is a homeomorphism onto its image.

Next, we prove $\phi(\mathbb{A}_K)$ is closed in $\mathbb{A}_L$. Let $\phi_v : K_v \to \prod_{w|v} L_w$. This has a closed image since K_v is complete and $\prod_{w|v} L_w$ is Hausdorff.

$\mathbb{A}_K = \{(x_v) \in \prod_v K_v \mid x_v \in \mathcal{O}_v \text{ for almost all } v\}$.

$\phi(\mathbb{A}_K) = \{(y_w) \in \mathbb{A}_L \mid \forall v, \exists x_v \in K_v \text{ s.t. } y_w = x_v \text{ for all } w|v\}$.

This is an intersection of closed sets $\bigcap_v C_v$ where $C_v = \{(y_w) \in \mathbb{A}_L \mid y_w \text{ is constant for } w|v\}$. Thus $\phi(\mathbb{A}_K)$ is closed.

(b) We prove a general version. If A is a topological K-algebra, L a finite extension of K. Then given basis $e_1, \dots, e_n$ of L/K, $A_L \cong A_K^n$. The product topology on A_L is independent of the choice of basis.

Assume $L = \bigoplus Ke_i = \bigoplus Kf_i$. Then $(e_1, \dots, e_n)A = (f_1, \dots, f_n)$ for some $A = (a_{ij}) \in GL_n(K)$.

Let $G_1 = (A_L, T_e)$ and $G_2 = (A_L, T_f)$ be the topological groups corresponding to the bases $\{e_i\}$ and $\{f_i\}$.

The map $\phi : G_1 \to A^n$ given by $\sum x_i e_i \mapsto (x_i)$ is a homeomorphism. The map $\psi : G_2 \to A^n$ given by $\sum y_j f_j \mapsto (y_j)$ is a homeomorphism.

The change of basis is given by $f_j = \sum_i a_{ij} e_i$. An element $z = \sum y_j f_j = \sum_j y_j (\sum_i a_{ij} e_i) = \sum_i (\sum_j a_{ij} y_j) e_i$.

So $x_i = \sum_j a_{ij} y_j$. This is multiplication by matrix A. The map $\mathbb{A}_K^n \to \mathbb{A}_K^n$, $(y_j) \mapsto (x_i)$ is a homeomorphism since multiplication and addition are continuous in $\mathbb{A}_K$.

Thus $T_e = T_f$, the topology is well-defined.

(c)

Lemma 3.5. For L/K a finite extension, K_v a local field, then $L \otimes_K K_v \cong \prod_{w|v} L_w$ as topological rings, where the RHS has the product topology.

The lemma is proved last semester.

Lemma 3.6. Let $w_1, \ldots, w_n$ be an integral basis for L/K, then for all but finite v, we have $\mathcal{O}_v w_1 \oplus \cdots \oplus \mathcal{O}_v w_n \leftrightarrow \prod_{w|v} \mathcal{O}_w$ under the above isomorphism.

Proof. LHS $\subseteq$ RHS since $v \in \mathcal{O}_w$, b_i for almost all w.

To get the inclusion the other way, we use the discriminant defined on the finite-dimensional K_v-algebra $A_v = L \otimes_K K_v$. Let $\gamma_1, \ldots, \gamma_N \in A_v$. The discriminant is given by

$$D(\gamma_1, \ldots, \gamma_N) = \det_{m,n} \Big(\mathrm{Tr}_{A_v/K_v}(\gamma_m \gamma_n) \Big).$$

Under the canonical isomorphism $A_v \cong \prod_{w|v} L_w$, we identify an element $\gamma \in A_v$ with its vector of components $(\gamma^{(w)})_{w|v}$, where $\gamma^{(w)} \in L_w$.

The trace map on the algebra A_v decomposes as the sum of the local traces relative to K_v. Specifically, for any γ_m, γ_n, we have the identity:

$$\mathrm{Tr}_{A_v/K_v}(\gamma_m \gamma_n) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v} \left(\gamma_m^{(w)} \gamma_n^{(w)} \right). \tag{1}$$

Now, assume that $\gamma_1, \ldots, \gamma_N$ are in the RHS, i.e.,

$$\gamma_n \in \prod_{w|v} \mathcal{O}_w.$$

This implies that for each w, the component $\gamma_n^{(w)}$ lies in the ring of integers $\mathcal{O}_w$ of the local field L_w. Since $\mathcal{O}_w$ is a ring, the product $\gamma_m^{(w)} \gamma_n^{(w)}$ is also in $\mathcal{O}_w$.

Recall that the local trace of an algebraic integer is an integer in the base local field. Therefore,

$$\mathrm{Tr}_{L_w/K_v} \left(\gamma_m^{(w)} \gamma_n^{(w)} \right) \in \mathcal{O}_v.$$

It follows from equation (1) that the total trace $\mathrm{Tr}_{A_v/K_v}(\gamma_m \gamma_n)$ is a sum of elements in $\mathcal{O}_v$, and thus lies in $\mathcal{O}_v$. Consequently, the determinant $D(\gamma_1, \ldots, \gamma_N)$ belongs to $\mathcal{O}_v$.

Now suppose that β is an element of the RHS, i.e.,

$$\beta \in \prod_{w|v} \mathcal{O}_w.$$

Since $\omega_1, \ldots, \omega_N$ is a basis for L/K, the set $\{1 \otimes \omega_1, \ldots, 1 \otimes \omega_N\}$ forms a basis for the algebra $A_v = L \otimes_K K_v$ over K_v. Thus, we can uniquely write

$$\beta = \sum_{n=1}^{N} b_n \omega_n \quad \text{with } b_n \in K_v.$$

We wish to show that for almost all v, the coefficients b_n actually lie in $\mathcal{O}_v$.

Consider the discriminant of the set of elements where the m-th basis vector ω_m is replaced by β. Using the multilinearity and the transformation property of the discriminant (which transforms by the square of the determinant of the change-of-basis matrix), we have:

$$D(\omega_1, \ldots, \omega_{m-1}, \beta, \omega_{m+1}, \ldots, \omega_N) = b_m^2 D(\omega_1, \ldots, \omega_N).$$

Let $d = D(\omega_1, \ldots, \omega_N)$. Note that $d \in K$ is the global discriminant of the basis.

Since we assumed $\beta \in \prod_{w|v} \mathcal{O}_w$, and we know that $\omega_n \in \prod_{w|v} \mathcal{O}_w$ for almost all v (as they are global integers), all the arguments inside the discriminant on the left-hand side lie in $\prod_{w|v} \mathcal{O}_w$. By the result established in the first part of the proof, this implies that the value of the discriminant lies in $\mathcal{O}_v$. Therefore,

$$b_m^2 d \in \mathcal{O}_v \quad (1 \leq m \leq N).$$

Since $\omega_1, \ldots, \omega_N$ is a basis, we have $d \neq 0$. For almost all normalized valuations v, we have $|d|_v = 1$ (i.e., d is a unit in $\mathcal{O}_v$). For such v, the condition $b_m^2 d \in \mathcal{O}_v$ implies

$$b_m^2 \in \mathcal{O}_v.$$

Since $\mathcal{O}_v$ is integrally closed in K_v, $b_m^2 \in \mathcal{O}_v$ implies $b_m \in \mathcal{O}_v$ (alternatively, in terms of valuation, $2v(b_m) \geq 0 \implies v(b_m) \geq 0$).

Thus, for almost all v, we have $b_m \in \mathcal{O}_v$ for all $1 \leq m \leq N$. This means

$$\beta = \sum_{n=1}^{N} b_n \omega_n \in \bigoplus_{n=1}^{N} \mathcal{O}_v \omega_n,$$

which proves that RHS $\subset$ LHS for almost all v.

Combining this with the easy inclusion LHS $\subset$ RHS, the lemma is proved. □

Proof of $L \otimes_K \mathbb{A}_K \cong \mathbb{A}_L$:

Let $e_1, \ldots, e_n$ be a basis for L/K. Algebraically, the tensor product decomposes as a direct sum:

$$L \otimes_K \mathbb{A}_K \cong \left(\bigoplus_{i=1}^{n} K e_i \right) \otimes_K \mathbb{A}_K \cong \bigoplus_{i=1}^{n} \mathbb{A}_K e_i.$$

Topologically, this is the restricted direct product of the local spaces $\bigoplus_{i=1}^{n} K_v e_i$ with respect

to the lattices $\bigoplus_{i=1}^n \mathcal{O}_v e_i$:

$$\text{LHS} \cong \prod_{v \in V_K}{}' \left(\bigoplus_{i=1}^n K_v e_i \right) \quad \text{w.r.t.} \quad \left(\bigoplus_{i=1}^n \mathcal{O}_v e_i \right).$$

For each place v, we have the canonical local isomorphism:

$$\phi_v : \bigoplus_{i=1}^n K_v e_i \cong K_v \otimes_K L \xrightarrow{\sim} \prod_{w|v} L_w.$$

By the previous Lemma, for almost all v, the lattice generated by the basis coincides with the integral closure:

$$\bigoplus_{i=1}^n \mathcal{O}_v e_i = \prod_{w|v} \mathcal{O}_w.$$

Thus, the restricted product conditions on both sides are identical for almost all v. We can regroup the product over v into a product over w:

$$\text{LHS} \cong \prod_{v \in V_K}{}' \left(\prod_{w|v} L_w \right) \text{ w.r.t. } \left(\prod_{w|v} \mathcal{O}_w \right) \cong \prod_{w \in V_L}{}' L_w \text{ w.r.t. } \mathcal{O}_w = \mathbb{A}_L.$$

□

Homework 3.4. (a) Show that the natural map $\mathbb{I}_K \to \mathbb{A}_K$ is continuous, but not a homeomorphism onto the image.

(b) The map $\mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K$ given by $x \mapsto (x, x^{-1})$ is a homeomorphism onto the image.

Proof. (a) The map is the inclusion map $i : \mathbb{I}_K \to \mathbb{A}_K$. It is continuous if the preimage of any open set in $\mathbb{A}_K$ is open in $\mathbb{I}_K$. The topology on $\mathbb{I}_K$ is the subspace topology from $\mathbb{A}_K \times \mathbb{A}_K$ via $x \mapsto (x, x^{-1})$. An open set in $\mathbb{A}_K$ is of the form U. Its preimage $i^{-1}(U) = U \cap \mathbb{I}_K$. We need to check if this is open in $\mathbb{I}_K$.

A basis for the topology on $\mathbb{I}_K$ is given by sets $(U \times V) \cap \phi(\mathbb{I}_K)$ where U, V are open in $\mathbb{A}_K$ and $\phi(x) = (x, x^{-1})$. The preimage under ϕ is $U \cap V^{-1}$.

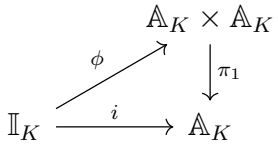
The inclusion $i : \mathbb{I}_K \to \mathbb{A}_K$ is continuous because it's the composition of $\phi : \mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K$ and the projection $\pi_1 : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$, both of which are continuous.

To show it's not a homeomorphism, we show the topology on $\mathbb{I}_K$ is strictly finer than the subspace topology from $\mathbb{A}_K$.

Consider the set $U = \{x \in \mathbb{I}_K \mid x_v \in \mathcal{O}_{K,v}^\times \text{ for all non-archimedean } v\}$. This is $\prod_v \mathcal{O}_{K,v}^\times$.

This set is open in $\mathbb{I}_K$. However, it is not open in the subspace topology. Any open ball in $\mathbb{A}_K$ around $1 \in U$ contains elements not in U. For example, take a basic open set $W = \prod_{v \in S} W_v \times \prod_{v \notin S} \mathcal{O}_{K,v}$ in $\mathbb{A}_K$ containing 1. For any $v_0 \notin S$, we can find an element $x \in W$ with $x_{v_0} = \pi_{v_0}$ (a uniformizer), so $x_{v_0} \notin \mathcal{O}_{K,v_0}^\times$. Thus $x \notin U$. So $W \not\subseteq U$.

(b) Let $\phi : \mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K$ be the map $x \mapsto (x, x^{-1})$.



ϕ is continuous because its components, $x \mapsto x$ and $x \mapsto x^{-1}$, are continuous maps from $\mathbb{I}_K$ to $\mathbb{A}_K$.

The map ϕ is a homeomorphism onto its image $\phi(\mathbb{I}_K)$ if its inverse $\psi : \phi(\mathbb{I}_K) \to \mathbb{I}_K$ is continuous.

The image $\phi(\mathbb{I}_K)$ is a subspace of $\mathbb{A}_K \times \mathbb{A}_K$. The inverse map is simply the projection onto the first coordinate, $\psi((x, y)) = x$.

The projection $\pi_1 : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$ is continuous. The restriction of a continuous map to a subspace is continuous. So $\psi = \pi_1|_{\phi(\mathbb{I}_K)}$ is continuous from $\phi(\mathbb{I}_K)$ (with subspace topology) to $\mathbb{A}_K$.

The target space is $\mathbb{I}_K$, not $\mathbb{A}_K$. We need to show that $\psi : \phi(\mathbb{I}_K) \to \mathbb{I}_K$ is continuous.

A basic open set in $\mathbb{I}_K$ is $U = W_1 \cap W_2^{-1}$ where W_1, W_2 are open in $\mathbb{A}_K$.

$\psi^{-1}(U) = \{(x, x^{-1}) \mid x \in U\} = \{(x, x^{-1}) \mid x \in W_1, x^{-1} \in W_2\}$.

This is equal to $\phi(W_1 \cap W_2^{-1}) = (W_1 \times W_2) \cap \phi(\mathbb{I}_K)$.

This is an open set in the subspace topology of $\phi(\mathbb{I}_K)$.

Therefore, ψ is continuous. Thus, ϕ is a homeomorphism onto its image. □

4 2024.9.25

Fact: For any measurable $B \subseteq \mathbb{A}_K$ and $g \in \mathbb{A}_K^*$, $\mu(gB) = \|g\|\mu(B)$.

Recall: $\forall v \in V_k$, Haar measure μ_v on K_v is normalized by $\mu_v(O_v) = 1$.

Fact: $K \hookrightarrow \mathbb{A}_K$ is discrete and hence closed. The Haar measure μ on $\mathbb{A}_K$ induces a Haar measure $\bar{\mu}$ on $\mathbb{A}_K/K$. (In particular, $\overline{\mu}(\mathbb{A}_K/K) < \infty$).

Let $V_k = S \subseteq V_k$, S finite set. Let $C := \prod_{v\in S} C_v \times \prod_{v\notin S} \mathcal{O}_{K_v} \subseteq \mathbb{A}_K$. C_v: closed disk on K_v. If $\mu(C) > \overline{\mu}(\mathbb{A}_K/K)$, then the natural map $C \hookrightarrow \mathbb{A}_K \to \mathbb{A}_K/K$ is NOT injective. (The fact is essential to many conclusions later.)

4.1 Adelic Minkowski Theorem

Recall: (Minkowski's Lem) $\Lambda \subseteq \mathbb{R}^n$ a lattice and $X \subseteq \mathbb{R}^n$ centrally symmetric convex region of finite measure. Assume $\mathrm{vol}(X) > 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. Then $\Lambda \cap X \neq \{0\}$.

Replace $\mathbb{R}^n$ by $\mathbb{A}_K$. Lattice Λ by K. discrete.

Replace X by $X_x \subseteq \mathbb{A}_K$ of "good shape" (such as C).

Definition 4.1. For all $x = (x_v)_v \in \mathbb{I}_K = \mathbb{A}_K^*$:

$$X_x := \{y \in \mathbb{A}_K \mid \|y_v\|_v \leq \|x_v\|_v, \forall v\}$$

Remark: X_x is of the form of C before.

Theorem 4.1 (Adelic Minkowski's Theorem). There exists a constant $C_K > 0$, depending only on the field K, such that for all $x \in \mathbb{I}_K$, if the idele norm $\|x\| > C_K$, then

$$X_x \cap K \neq \{0\}$$

Proof. Let $Z = \left\{z \in \mathbb{A}_K \mid \forall v \in V_{K,\infty}, |z_v|_v \leq \frac{1}{2} \text{ and } \forall v \in V_{K,f}, \|z_v\|_v \leq 1\right\}$.

Let the constant $c = C_K := \frac{\bar{\mu}(\mathbb{A}_K/K)}{\mu(Z)}$.

For any $x \in \mathbb{I}_K$ such that $\|x\| > c$, we have

$$\mu(xZ) = \|x\|\mu(Z) > c \cdot \mu(Z) = \frac{\overline{\mu}(\mathbb{A}_K/K)}{\mu(Z)}\mu(Z) = \overline{\mu}(\mathbb{A}_K/K).$$

Apply the fact before: since $\mu(xZ) > \overline{\mu}(\mathbb{A}_K/K)$, the natural map $xZ \to \mathbb{A}_K/K$ is not injective. Therefore, there exist $y, y' \in xZ$ with $y \neq y'$ such that they have the same image in $\mathbb{A}_K/K$. This means their difference is a non-zero element of K. Let $a = y - y' \in K \setminus \{0\}$.

It remains to show that $a \in X_x$. Since $y, y' \in xZ$, we can write $y = xz$ and $y' = xz'$ for some $z, z' \in Z$. Then $a = y - y' = x(z - z')$.

For any place v, we have

$$\|a_v\|_v = \|x_v(z_v - z'_v)\|_v = \|x_v\|_v \|z_v - z'_v\|_v.$$

By the definition of Z, if v is an infinite place, $\|z_v - z'_v\|_v \leq |z_v|_v + |z'_v|_v \leq \frac{1}{2} + \frac{1}{2} = 1$. If v is a finite place, $\|z_v - z'_v\|_v \leq \max(\|z_v\|_v, \|z'_v\|_v) \leq 1$. Thus, for all places v, $\|z_v - z'_v\|_v \leq 1$.

Therefore, for all v,

$$\|a_v\|_v \leq \|x_v\|_v \cdot 1 = \|x_v\|_v.$$

This shows that $a \in X_x$ by definition. □

4.2 Application of Adelic Minkowski

Proposition 4.1 (**Weak Approximation Theorem**). Let $v_1, \ldots, v_r \in V_K$ be distinct places. Then the diagonal embedding

$$K \hookrightarrow \prod_{i=1}^{r} K_{v_i}$$

has a dense image. (i.e., for all $(a_1, \ldots, a_r) \in \prod_{i=1}^r K_{v_i}$ and for all $\epsilon > 0$, there exists an element $x \in K$ such that $\|x - a_i\|_{v_i} < \epsilon$ for all $i \in \{1, \ldots, r\}$).

Theorem 4.2 (**Strong Approximation Theorem**). Let $v_0 \in V_K$ be a place. Define the adele ring without the v_0 component as

$$\mathbb{A}_K^{v_0} = \prod_{v \neq v_0}{}' K_v$$

with respect to the rings of integers $\mathcal{O}_{K_v} \subseteq K_v$ for all finite places $v \in V_{K,f} \setminus \{v_0\}$. Then the diagonal embedding $K \hookrightarrow \mathbb{A}_K^{v_0}$ has a dense image. (i.e., for all $a = (a_v) \in \mathbb{A}_K^{v_0}$, for any finite set of places $S \subseteq V_K \setminus \{v_0\}$, and for all $\epsilon > 0$, there exists an element $x \in K$ such that:

- $\|x - a_v\|_v < \epsilon$ for all $v \in S$.
- $\|x - a_v\|_v \leq 1$ for all $v \in V_K \setminus (S \cup \{v_0\})$).

Proof. **Step 1. Claim: There exists an idele $w_0 \in \mathbb{I}_K$ such that $X_{w_0} + K = \mathbb{A}_K$.**

Define the set X_w^o for an idele $w \in \mathbb{I}_K$ as

$$X_w^o := \{x \in \mathbb{A}_K \mid \|x_v\|_v < \|w_v\|_v \text{ for all } v \in V_{K,\infty} \text{ and } \|x_v\|_v \leq \|w_v\|_v \text{ for all } v \in V_{K,f}\}.$$

We note the following facts:

- Each set $X_w^o \subseteq \mathbb{A}_K$ is open.
- The collection of these sets covers the adele ring: $\mathbb{A}_K = \bigcup_{w \in \mathbb{I}_K} X_w^o$.
- The quotient space $\mathbb{A}_K/K$ is compact.
- The canonical projection map $\mathbb{A}_K \to \mathbb{A}_K/K$ is an open map.

From the properties of the quotient map $\mathbb{A}_K \to \mathbb{A}_K/K$ and the compactness of $\mathbb{A}_K/K$, the open cover $\{(X_w^o + K)/K\}_{w \in \mathbb{I}_K}$ has a finite subcover.

$$\implies \exists w_1, \ldots, w_r \in \mathbb{I}_K \text{ s.t. } \mathbb{A}_K = \bigcup_{i=1}^{r} (X_{w_i}^o + K).$$

We can then easily choose a single idele $w \in \mathbb{I}_K$ such that $\bigcup_{i=1}^r X_{w_i}^o \subseteq X_w^o$. This gives $\mathbb{A}_K = X_w^o + K$.

Step 2: Find x with desired properties.

We may enlarge the finite set S to contain $V_{K,\infty}$. Let $a \in \mathbb{A}_K^{v_0}$ and $\epsilon > 0$ be given.

By the Adelic Minkowski theorem, for any idele $w' \in \mathbb{I}_K$ with norm $\|w'\| > C_K$, the intersection $X_{w'}^o \cap K$ is non-empty. So, we can find a non-zero element $u \in X_{w'}^o \cap K$.

Consider the element $au^{-1} \in \mathbb{A}_K$. From Step 1, we know $\mathbb{A}_K = X_w^o + K$, so we can write

$$au^{-1} = \alpha + \beta, \quad \text{for some } \alpha \in K, \beta \in X_w^o.$$

This implies $a = \alpha u + \beta u$. Let $x = \alpha u \in K$. Then $a - x = \beta u$.

It remains to show that x is the desired approximation by choosing w' appropriately. We need to show:

$$\|\beta u\|_v < \epsilon, \quad \forall v \in S$$

$$\|\beta u\|_v \leq 1, \quad \forall v \notin S \cup \{v_0\}$$

We have the bound $\|\beta_v u_v\|_v = \|\beta_v\|_v \|u_v\|_v \leq \|w_v\|_v \|u_v\|_v$ since $\beta \in X_w^o$. And since $u \in X_{w'}^o$, we have $\|u_v\|_v \leq \|w'_v\|_v$. So, $\|a_v - x_v\|_v \leq \|w_v\|_v \|w'_v\|_v$.

We may choose the components of our idele w' as follows:

- For the finitely many places $v \in S$, choose $\|w'_v\|_v$ small enough such that $\|w_v\|_v \|w'_v\|_v < \epsilon$.
- For other places $v \notin S \cup \{v_0\}$, choose $\|w'_v\|_v$ such that $\|w_v\|_v \|w'_v\|_v \leq 1$. (e.g., choose $\|w'_v\|_v = 1$ where $\|w_v\|_v \leq 1$).

To ensure that $\|w'\| = \prod_v \|w'_v\|_v > C_K$, we must choose the component at the remaining place v_0 to be large enough. This is possible, and with such a w', the resulting $x \in K$ is the required approximation. □

Recall:

- The embedding $K \hookrightarrow \mathbb{A}_K$ has a discrete image.
- The multiplicative group of the field embeds into the idele group: $K^\times \hookrightarrow \mathbb{I}_K = \mathbb{A}_K^\times$.
- The idele norm is a continuous homomorphism $\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}$ defined by

$$x = (x_v)_v \mapsto \|x\| = \prod_v \|x_v\|_v.$$

- The idele norm can be extended to a function $\|\cdot\| : \mathbb{A}_K \to \mathbb{R}_{\geq 0}$.

Let $\mathbb{I}_K^1$ be the group of ideles of norm 1.

$$\mathbb{I}_K^1 := (\mathbb{A}_K^\times)^1 := \ker\left(\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}\right)$$

By the product formula, the image of $K^\times$ is contained in $\mathbb{I}_K^1$.

$$K^\times \hookrightarrow \mathbb{I}_K^1 \subseteq \mathbb{I}_K = \mathbb{A}_K^\times$$

The embedding of $K^\times$ into $\mathbb{I}_K$ has a discrete image, which implies that $K^\times$ is also a discrete subgroup of $\mathbb{I}_K^1$.

Theorem 4.3. The topological group $\mathbb{I}_K^1/K^\times$ is compact.

Remark: We have previously proved this result for the case $K = \mathbb{Q}$, where we showed the isomorphism $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times \cong \prod_p \mathbb{Z}_p^\times$, which is compact.

Lemma 4.1. The following statements hold:

1. The subset $\mathbb{I}_K^1 \subseteq \mathbb{A}_K$ is closed.
2. The topology on $\mathbb{I}_K^1$ (i.e., the subspace topology inherited from $\mathbb{I}_K$) agrees with the subspace topology inherited from $\mathbb{A}_K$.

Proof Sketch of Theorem from Lemma. The lemma implies that to prove the theorem, it is sufficient to find a compact set $E \subseteq \mathbb{A}_K$ such that the intersection $E \cap \mathbb{I}_K^1$ maps surjectively

onto the quotient group $\mathbb{I}_K^1/K^\times$ under the canonical projection. (This uses properties (1) and (2) from the lemma).

Let us choose $E = X_x$ for some idele $x \in \mathbb{I}_K$. The set X_x is compact. We want to find an $x \in \mathbb{I}_K$ such that the map $X_x \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$ is surjective. This is equivalent to the statement:

$$\mathbb{I}_K^1 = (X_x \cap \mathbb{I}_K^1) \cdot K^\times$$

To show this, for any given idele $y \in \mathbb{I}_K^1$, we need to find a principal idele $r \in K^\times$ such that $r^{-1}y \in X_x \cap \mathbb{I}_K^1$. The condition $r^{-1}y \in \mathbb{I}_K^1$ is automatically satisfied since $\|r^{-1}y\| = \|r\|^{-1}\|y\| = 1 \cdot 1 = 1$. So we only need to ensure $r^{-1}y \in X_x$.

This is equivalent to finding a non-zero element $r \in K$ such that $r \in X_{x/y}$. By the Adelic Minkowski theorem, such an element r exists if the "volume" of $X_{x/y}$ is sufficiently large. The volume is proportional to the norm $\|x/y\|$. Since $y \in \mathbb{I}_K^1$, we have $\|y\| = 1$, so $\|x/y\| = \|x\|/\|y\| = \|x\|$.

Therefore, we can choose a fixed idele $x \in \mathbb{I}_K$ such that its norm $\|x\|$ is greater than the Minkowski constant C_K. Then for any $y \in \mathbb{I}_K^1$, we have $\|x/y\| = \|x\| > C_K$. By Adelic Minkowski, the set $X_{x/y} \cap K$ contains a non-zero element, which we call r. This r is in $K^\times$.

The existence of such an $r \in K^\times$ for any $y \in \mathbb{I}_K^1$ implies that $yr \in X_x$. Since $\|yr\| = \|y\|\|r\| = 1 \cdot 1 = 1$, we have $yr \in X_x \cap \mathbb{I}_K^1$. This means that the image of $X_x \cap \mathbb{I}_K^1$ under the projection map covers the entire space $\mathbb{I}_K^1/K^\times$. Since X_x is compact and $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$ (by the lemma below), the intersection $X_x \cap \mathbb{I}_K^1$ is compact. The continuous image of a compact set is compact, so $\mathbb{I}_K^1/K^\times$ is compact. □

Proof of Lemma. **Key observation:** For any finite place $v \in V_{K,f}$, the norm is discrete. If $\|x_v\|_v < 1$, then $\|x_v\|_v \leq 1/q_v$, where q_v is the size of the residue field, which is at least 2. So $\|x_v\|_v \leq 1/2$.

(1) We want to show that $\mathbb{A}_K \setminus \mathbb{I}_K^1$ is an open set. This is equivalent to showing that for any $x \in \mathbb{A}_K$ with $\|x\| \neq 1$, there is an open neighborhood of x that is disjoint from $\mathbb{I}_K^1$. We can extend the idele norm to a function $\|\cdot\| : \mathbb{A}_K \to \mathbb{R}_{\geq 0}$. If $x = (x_v) \in \mathbb{A}_K$ has infinitely many components x_v that are not units in their respective local rings $\mathcal{O}_{K_v}$, then $\|x\| = 0$.

Case 1: $\|x\| < 1$**.**

Let S be a finite set of places containing all infinite places $V_{K,\infty}$ and all finite places where $x_v \notin \mathcal{O}_{K_v}$. For any y in a sufficiently small neighborhood of x, we will have $y_v \in \mathcal{O}_{K_v}$ for $v \notin S$.

More simply, let's choose a finite set $S \supseteq V_{K,\infty}$ large enough so that for $v \notin S$, we have $x_v \in \mathcal{O}_{K_v}$ and $\prod_{v \in S} \|x_v\|_v$ is close to $\|x\| < 1$.

We can choose open neighborhoods U_v of x_v for $v \in S$ such that for any $y_v \in U_v$,

$$\prod_{v \in S} \|y_v\|_v < 1$$

Let $U = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}$. This is an open neighborhood of x. For any $y \in U$, we have

$$\|y\| = \left(\prod_{v \in S} \|y_v\|_v\right) \left(\prod_{v \notin S} \|y_v\|_v\right) \leq \prod_{v \in S} \|y_v\|_v < 1.$$

Thus, this open neighborhood U is disjoint from $\mathbb{I}_K^1$.

Case 2: $\|x\| = p > 1$**.**

We can choose a finite set of places $S \subseteq V_K$ containing:

1. all infinite places, $V_{K,\infty} \subseteq S$.
2. all finite places $v \in V_{K,f}$ where $\|x_v\|_v \neq 1$.
3. all finite places $v \in V_{K,f}$ where the residue field k_v has less than $2p$ elements.

Since for any $v \notin S$, we have $\|x_v\|_v = 1$, the product of norms over these places is 1. Then the total norm is given by the product over S:

$$\prod_{v \in S} \|x_v\|_v = \|x\| = p > 1.$$

For each $v \in S$, we can choose an open neighborhood U_v of x_v such that for any $y_v \in U_v$, the product of their norms remains greater than 1. For instance, such that $\prod_{v \in S} \|y_v\|_v \in (1, 2p)$.

Let $U := \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}$. This is an open neighborhood of x in $\mathbb{A}_K$. It remains to show that $U \cap \mathbb{I}_K^1 = \emptyset$.

For any $y \in U$, its norm is $\|y\| = \left(\prod_{v \in S} \|y_v\|_v\right) \left(\prod_{v \notin S} \|y_v\|_v\right)$. By construction, for any $y \in U$, we have $\prod_{v \in S} \|y_v\|_v \in (1, 2p)$. Also, for $v \notin S$, we have $y_v \in \mathcal{O}_{K_v}$, which implies $\|y_v\|_v \leq 1$. So, $\prod_{v \notin S} \|y_v\|_v \leq 1$. Therefore, $\|y\| = \left(\prod_{v \in S} \|y_v\|_v\right) \left(\prod_{v \notin S} \|y_v\|_v\right) < 2p \cdot 1 = 2p$.

If $y_v \in \mathcal{O}_{K_v}^\times$ for all $v \notin S$, then $\prod_{v \notin S} \|y_v\|_v = 1$. In this case, $\|y\| = \prod_{v \in S} \|y_v\|_v \in (1, 2p)$, so $\|y\| \neq 1$.

If there exists some $v_0 \notin S$ such that $y_{v_0} \in \mathcal{O}_{K_{v_0}} \setminus \mathcal{O}_{K_{v_0}}^\times$, then $\|y_{v_0}\|_v < 1/2p$. Then the total norm is $\|y\| = \left(\prod_{v \in S} \|y_v\|_v\right) \left(\prod_{v \notin S} \|y_v\|_v\right) < 2p \cdot \frac{1}{2p} = 1$.

So in any subcase, the norm of an element $y \in U$ cannot be exactly 1. Thus $U \cap \mathbb{I}_K^1 = \emptyset$. This completes the proof that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$.

(2) Proof of the second statement (equivalence of topologies). It suffices to show that for any $x \in \mathbb{I}_K^1$, there is a family of subsets of $\mathbb{I}_K^1$ which is a neighborhood basis in both the topology inherited from $\mathbb{A}_K$ and the topology inherited from $\mathbb{I}_K$.

Consider:

$$V = \left(\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times \right)$$

$$U = \left(\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v} \right)$$

where S is any finite set of places containing $V_{K,\infty}$ such that for any $v \notin S$, $x_v \in \mathcal{O}_{K_v}^\times$. And the neighborhoods $x_v \in U_v$ for $v \in S$ to be small enough such that for any $y_v \in U_v$, the product of norms is controlled, e.g., $\prod_{v \in S} \|y_v\|_v \in [2/3, 4/3]$.

Then such sets U form a neighborhood basis of x in $\mathbb{A}_K$, and such sets V form a neighborhood basis of x in $\mathbb{I}_K$.

It remains to show that $U \cap \mathbb{I}_K^1 = V \cap \mathbb{I}_K^1$.

The inclusion $V \cap \mathbb{I}_K^1 \subseteq U \cap \mathbb{I}_K^1$ is obvious since $V \subseteq U$.

For the other direction, let $y = (y_v) \in U \cap \mathbb{I}_K^1$. We want to show that $y_v \in \mathcal{O}_{K_v}^\times$ for all $v \notin S$. By definition of U, we have $y_v \in \mathcal{O}_{K_v}$ for all $v \notin S$. Suppose for contradiction that there exists a place $v_0 \notin S$ such that y_{v_0} is not a unit, i.e., $\|y_{v_0}\|_{v_0} < 1$. Since v_0 is a finite place, this implies $\|y_{v_0}\|_{v_0} \leq 1/2$.

The total norm of y is 1 since $y \in \mathbb{I}_K^1$.

$$1 = \|y\| = \left(\prod_{v \in S} \|y_v\|_v \right) \cdot \|y_{v_0}\|_{v_0} \cdot \left(\prod_{v \notin S \cup \{v_0\}} \|y_v\|_v \right)$$

By construction, $\prod_{v \in S} \|y_v\|_v < 4/3$. For all other places $v \notin S \cup \{v_0\}$, we have $\|y_v\|_v \leq 1$. This leads to the contradiction:

$$1 = \|y\| \leq \left(\frac{4}{3} \right) \cdot \left(\frac{1}{2} \right) \cdot 1 = \frac{2}{3} < 1.$$

This is impossible. Therefore, our assumption was false, and for all $v \notin S$, we must have $\|y_v\|_v = 1$, which means $y_v \in \mathcal{O}_{K_v}^\times$. This shows that $y \in V$, so $U \cap \mathbb{I}_K^1 \subseteq V \cap \mathbb{I}_K^1$. □

Remark: Connection to Ideal Class Group

Let $V_{K,\infty} \subseteq S \subseteq V_K$ be a finite set of places. The **ring of S-integers** is defined as:

$$\mathcal{O}_{K,S} := \{x \in K \mid \|x\|_v \leq 1 \text{ for all } v \notin S\}$$

It is a Dedekind domain with fractional field K. Its prime ideals are in bijection with the set of places $V_K \setminus S$.

The **ideal class group** of $\mathcal{O}_{K,S}$ is the quotient group

$$\mathrm{Cl}(\mathcal{O}_{K,S}) := \frac{\{\text{group of fractional ideals}\}}{\{\text{group of principal ideals}\}}$$

When $S = V_{K,\infty}$, then $\mathcal{O}_{K,S} = \mathcal{O}_K$ is the usual ring of integers of K, and $\mathrm{Cl}(\mathcal{O}_{K,S}) = \mathrm{Cl}(\mathcal{O}_K)$ is the class group of K.

There is a surjective group homomorphism from the idele group to the ideal class group:

$$\phi : \mathbb{I}_K \to \mathrm{Cl}(\mathcal{O}_{K,S})$$

defined by

$$(x_v)_v \mapsto \left[\prod_{v \notin S} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}\right]$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to the place v, and $[I]$ denotes the class of the ideal I.

Remark: The kernel of the homomorphism $\phi : \mathbb{I}_K \to \mathrm{Cl}(\mathcal{O}_{K,S})$ is given by

$$\ker(\phi) = K^\times \cdot \mathbb{I}_{K,S}$$

where $\mathbb{I}_{K,S} := \{x \in \mathbb{I}_K \mid \|x_v\|_v = 1 \text{ for all } v \notin S\}$. (Proof omitted).

Fact:

1. The ideal class group $\mathrm{Cl}(\mathcal{O}_{K,S})$ is a finite group.
2. The group of S-units $\mathcal{O}_{K,S}^\times$ is a finitely generated abelian group of rank $|S| - 1$. (This is Dirichlet's S-unit theorem).

4.3 The Idele Class Group

Definition 4.2. The **idele class group** of a number field K is the quotient group

$$C_K := \mathbb{I}_K / K^\times$$

Remark: For the field of rational numbers $K = \mathbb{Q}$, the idele class group is isomorphic to

$$C_{\mathbb{Q}} \cong \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times$$

where $\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ is the group of units of the ring of profinite integers.

The idele norm $\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}$ is a continuous homomorphism. Since $K^\times \subseteq \ker(\|\cdot\|) = \mathbb{I}_K^1$, the norm map descends to a continuous homomorphism on the idele class group:

$$\|\cdot\| : C_K \to \mathbb{R}_{>0}$$

The kernel of this map is the **norm-1 idele class group**, denoted C_K^1.

$$C_K^1 := \mathbb{I}_K^1/K^\times = \ker(\|\cdot\| : C_K \to \mathbb{R}_{>0})$$

We have previously shown that C_K^1 is a compact group. For $K = \mathbb{Q}$, we have $C_{\mathbb{Q}}^1 \cong \hat{\mathbb{Z}}^\times$.

Remark: The idele class group C_K is a Hausdorff topological group. This is because $K^\times$ is a discrete and therefore closed subgroup of $\mathbb{I}_K$.

There exists a continuous group homomorphism $s : \mathbb{R}_{>0} \to \mathbb{I}_K$ which is a section of the norm map, i.e., $\|s(a)\| = a$ for all $a \in \mathbb{R}_{>0}$. To define this, we fix an infinite place $v_0 \in V_{K,\infty}$.

- If $K_{v_0} = \mathbb{R}$, we define the section $s : \mathbb{R}_{>0} \to \mathbb{I}_K$ by

$$a \mapsto (x_v)_v \quad \text{where} \quad x_{v_0} = a \text{ and } x_v = 1 \text{ for all } v \neq v_0.$$

- If $K_{v_0} = \mathbb{C}$, we define the section $s : \mathbb{R}_{>0} \to \mathbb{I}_K$ by

$$a \mapsto (x_v)_v \quad \text{where} \quad x_{v_0} = \sqrt{a} \text{ and } x_v = 1 \text{ for all } v \neq v_0.$$

(Note that for $z \in \mathbb{C}$, $\|z\|_{v_0} = |z|^2$, so $\|\sqrt{a}\|_{v_0} = |\sqrt{a}|^2 = a$).

This section gives an isomorphism of topological groups:

$$\mathbb{I}_K \cong \mathbb{I}_K^1 \times \mathbb{R}_{>0}$$

Taking the quotient by $K^\times$ (which is entirely contained in the $\mathbb{I}_K^1$ factor), we get a corresponding isomorphism for the idele class group:

$$C_K \cong C_K^1 \times \mathbb{R}_{>0}$$

This is an isomorphism of topological groups.

Recall: For a finite extension of number fields L/K, there are natural embeddings:

$$\mathbb{A}_K \hookrightarrow \mathbb{A}_L$$
$$\mathbb{I}_K \hookrightarrow \mathbb{I}_L$$
$$C_K \hookrightarrow C_L$$

Remark: The map $C_K \to C_L$ is injective. To show this, it suffices to show that $\mathbb{I}_K \cap L^\times = K^\times$ inside $\mathbb{I}_L$. This follows from the fact that there is a canonical isomorphism of topological rings $\mathbb{A}_K \otimes_K L \cong \mathbb{A}_L$.

Proposition 4.2. The natural map $i : C_K \hookrightarrow C_L$ is a closed embedding.

Exercise 4.1. Let $\|\cdot\|_K : \mathbb{I}_K \to \mathbb{R}_{>0}$ and $\|\cdot\|_L : \mathbb{I}_L \to \mathbb{R}_{>0}$ be the respective idele norms. Then for any idele $x \in \mathbb{I}_K$, its norm when viewed as an element of $\mathbb{I}_L$ is related by the degree of the extension:

$$\|x\|_L = \|x\|_K^{[L:K]}$$

Proof of Proposition (using the exercise). We have the following commutative diagram of short exact sequences of topological groups:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_K^1 & \longrightarrow & C_K & \xrightarrow{\|\cdot\|_K} & \mathbb{R}_{>0} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle (\cdot)^{[L:K]}} & & \\ 0 & \longrightarrow & C_L^1 & \longrightarrow & C_L & \xrightarrow{\|\cdot\|_L} & \mathbb{R}_{>0} & \longrightarrow & 0 \end{array}$$

Using the isomorphism $C_K \cong C_K^1 \times \mathbb{R}_{>0}$ (and similarly for L), the map $i : C_K \to C_L$ can be identified with the map:

$$i : C_K^1 \times \mathbb{R}_{>0} \to C_L^1 \times \mathbb{R}_{>0}$$

$$(c, t) \mapsto (i_1(c), t^{[L:K]})$$

We need to show this map is a closed embedding. An embedding is a continuous, injective map that is a homeomorphism onto its image (i.e., the inverse map from the image is continuous). For group homomorphisms, injectivity and continuity are often easier to establish; the main point is that the map is closed.

1. The map on the second component, $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ given by $t \mapsto t^{[L:K]}$, is a homeomorphism onto its image, and its image is closed if $[L : K] > 0$. Thus, it is a closed embedding.

2. The map on the first component, $i_1 : C_K^1 \to C_L^1$, is a continuous map from a compact space (C_K^1) to a Hausdorff space (C_L^1). Any such map is a closed map. Since it is also injective, it is a closed embedding.

Since the map i is a product of two closed embeddings, it is itself a closed embedding. □

Definition 4.3. Let L/K be a finite extension of number fields.

Recall: The definition of the field norm $N_{L/K} : L \to K$. For any element $x \in L$, we consider the multiplication-by-x map, $\phi_x : L \to L$, defined by $\phi_x(y) = xy$. This is a K-linear map of vector spaces. The norm of x is defined as the determinant of this map:

$$N_{L/K}(x) := \det(\phi_x).$$

We extend this definition to the adele rings. The **adelic norm map** is a continuous homomorphism $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$. For any $x \in \mathbb{A}_L$, we define the multiplication map $\tilde{\phi}_x : \mathbb{A}_L \to \mathbb{A}_L$ by

$$\tilde{\phi}_x(y) = xy.$$

Since $\mathbb{A}_L$ is a free module over $\mathbb{A}_K$ of rank $[L : K]$, the map $\tilde{\phi}_x$ is an $\mathbb{A}_K$-linear endomorphism. The adelic norm is defined as its determinant:

$$N_{L/K}(x) := \det(\tilde{\phi}_x).$$

This map restricts to a map on the ideles, $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$.

4.4 Homework

Homework 4.1. In the adelic Minkowski theorem, show that $c_{\mathbb{Q}} = 1$.

Proof. By the proof of Adelic Minkowski's theorem, $c_{\mathbb{Q}} = 1/\mu(Z)$, where

$$Z = \left\{ x \in \mathbb{A} \mid \|x_v\|_v \leq 1 \text{ for } v \notin V_{K,\infty}, \text{ and } \|x_v\|_v \leq \frac{1}{2} \text{ for } v \in V_{K,\infty} \right\}.$$

Since μ is normalized,

$$\mu(Z) = \mu_\infty([-1/2, 1/2]) \cdot \prod_{v \notin V_{K,\infty}} \mu_v(\mathcal{O}_v) = 1.$$

Thus $c_{\mathbb{Q}} = 1$. □

Homework 4.2. Let L/K be an extension of number fields. Write $\|\cdot\|_K : \mathbb{I}_K \to \mathbb{R}_{>0}$ and $\|\cdot\|_L : \mathbb{I}_L \to \mathbb{R}_{>0}$ for the idele norms respectively. Let $i : \mathbb{I}_K \to \mathbb{I}_L$ be the natural map. Show that for any $x \in \mathbb{I}_K$, we have $\|i(x)\|_L = \|x\|_K^{[L:K]}$.

Proof. For $x \in \mathbb{I}_K$,

$$\begin{aligned}
\|i(x)\|_L &= \prod_{w \in V_L} \|(i(x))_w\|_w \\
&= \prod_{w \in V_L} \|x_v\|_w \quad \text{where } v \in V_K \text{ such that } w \mid v \\
&= \prod_{w \in V_L} \|x_v\|_v^{[L_w : K_v]} \\
&= \prod_{v \in V_K} \prod_{w \mid v} \|x_v\|_v^{[L_w : K_v]} \\
&= \prod_{v \in V_K} \|x_v\|_v^{\sum_{w \mid v} [L_w : K_v]} \\
&= \prod_{v \in V_K} \|x_v\|_v^{[L:K]} \\
&= \|x\|_K^{[L:K]}.
\end{aligned}$$

□

Homework 4.3. Show that the following statements hold:

1. For any $x \in \mathbb{A}_L$, we have $x \in \mathbb{I}_L$ if and only if $N_{L/K}(x) \in \mathbb{I}_K$. In particular, we

have a group homomorphism $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$.

2. We have a commutative diagram

$$\begin{array}{ccc} L & \longrightarrow & \mathbb{A}_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K & \longrightarrow & \mathbb{A}_K \end{array}$$

3. For $w|v$, we have a commutative diagram

$$\begin{array}{ccc} L_w & \longrightarrow & \mathbb{A}_L \\ {\scriptstyle N_{L_w/K_v}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K_v & \longrightarrow & \mathbb{A}_K \end{array}$$

where $K_v \to \mathbb{A}_K$ denote the natural embedding to the v-th component. Similar for $L_w \to \mathbb{A}_L$.

4. For $x = (x_w)_w \in \mathbb{A}_L$, we have $N_{L/K}(x) = (y_v)_v$ with $y_v = \prod_{w \in V_L, w|v} N_{L_w/K_v}(x_w)$.

5. For $x \in \mathbb{I}_L$, we have $\|N_{L/K}(x)\|_K = \|x\|_L$.

6. For $x \in \mathbb{A}_K \subset \mathbb{A}_L$, $N_{L/K}(x) = x^{[L:K]}$.

Proof. For any $x \in \mathbb{A}_L$, consider $m_x : \mathbb{A}_L \to \mathbb{A}_L$ given by $y \mapsto xy$ as an $\mathbb{A}_K$-linear map. Since $\mathbb{A}_L$ is free of rank n over $\mathbb{A}_K$, we define $N_{L/K}(x) = \det(m_x) \in \mathbb{A}_K$. We first prove (d).

(d) Fix a place v of K. Consider taking base change of projection map $\pi_v : \mathbb{A}_K \to K_v$. Then $\mathbb{A}_L \otimes_{\mathbb{A}_K} K_v \cong L \otimes_K \mathbb{A}_K \otimes_{\mathbb{A}_K} K_v \cong L \otimes_K K_v \cong \prod_{w|v} L_w$ as K_v-algebras. Since taking determinant commutes with base change, we have

$$\pi_v(N_{L/K}(x)) = \pi_v(\det(m_x)) = \det(m_x \otimes \mathrm{id}_{K_v}).$$

Under the isomorphism $\mathbb{A}_L \otimes_{\mathbb{A}_K} K_v \cong \prod_{w|v} L_w$, the map $m_x \otimes \mathrm{id}_{K_v}$ corresponds to the K_v-linear map

$$M : \prod_{w|v} L_w \to \prod_{w|v} L_w, \quad (z_w)_{w|v} \mapsto (x_w z_w)_{w|v}.$$

Therefore,

$$(N_{L/K}(x))_v = \det(M) = \prod_{w|v} N_{L_w/K_v}(x_w).$$

(a) Since the determinant is multiplicative, $N_{L/K}$ is a group homomorphism. If $x \in \mathbb{I}_L$, then $N_{L/K}(x)N_{L/K}(x^{-1}) = N_{L/K}(1) = 1$. Thus $N_{L/K}(x) \in \mathbb{I}_K$.

Conversely, if $N_{L/K}(x) \in \mathbb{I}_K$, by (d), for all places v of K, we have $\prod_{w|v} N_{L_w/K_v}(x_w) \in K_v^\times$. Thus for all places w of L, $N_{L_w/K_v}(x_w) \neq 0$, so $x_w \in L_w^\times$ for all w. Moreover, for almost all v, we have

$$1 = \prod_{w|v} |N_{L_w/K_v}(x_w)|_v = \prod_{w|v} |x_w|_w^{[L_w:K_v]}. \tag{2}$$

For v satisfying (2), if there is some $w \mid v$ with $|x_w|_w < 1$, there must be some other $w' \mid v$ with $|x_{w'}|_{w'} > 1$, thus there are only finitely many such v because $x \in \mathbb{A}_L$. Therefore, for almost all w, we have $|x_w|_w = 1$. Hence, $x \in \mathbb{I}_L$.

(b) Let $i_K : K \hookrightarrow \mathbb{A}_K$ and $i_L : L \hookrightarrow \mathbb{A}_L$. Let $\alpha \in L$. By (d), for each v,

$$N_{L/K}(i_L(\alpha))_v = \prod_{w|v} N_{L_w/K_v}(\alpha) = N_{L/K}(\alpha),$$

Thus, $N_{L/K}(i_L(\alpha)) = i_K(N_{L/K}(\alpha))$.

(c) Let $x_w \in L_w$. Embed it into $\mathbb{A}_L$ as x with x_w at w and 1 elsewhere. Apply (d). For $v' \neq v$, $N_{L/K}(x)_{v'} = 1$. For $v' = v$, $N_{L/K}(x)_v = N_{L_w/K_v}(x_w)$. Thus, the diagram commutes.

(e) By (d), for $x \in \mathbb{I}_L$,

$$\begin{aligned}
\|N_{L/K}(x)\|_K &= \prod_v \|(N_{L/K}(x))_v\|_v \\
&= \prod_v \prod_{w|v} \|N_{L_w/K_v}(x_w)\|_v \\
&= \prod_w \|N_{L_w/K_v}(x_w)\|_w^{1/[L_w:K_v]} \\
&= \prod_w \|x_w\|_w = \|x\|_L.
\end{aligned}$$

(f) If $x \in \mathbb{A}_K$, by (d), $(N_{L/K}(x))_v = \prod_{w|v} N_{L_w/K_v}(x_v) = \prod_{w|v} x_v^{[L_w:K_v]} = x_v^{\sum_{w|v}[L_w:K_v]} = x_v^{[L:K]}$. □

5 2025.10.9

Recall: K is a number field.

$$\begin{aligned}
\mathbb{I}_K &= \prod_v{}' K_v^* \quad \text{restricted product of } O_{K_v}.\\
||\cdot|| : \mathbb{I}_K &\to \mathbb{R}_{>0}\\
(x_v)_v &\mapsto \prod_v ||x_v||_v. \quad \text{idele norm.}\\
\mathbb{I}_K^1 &:= \mathrm{Ker}(||\cdot||)\\
C_K &:= \mathbb{I}_K/K^* \quad \text{idele class group}\\
||\cdot|| : C_K &\to \mathbb{R}_{>0} \quad (\text{factor through } C_K)\\
C_K^1 &:= \mathrm{Ker}(C_K \xrightarrow{||\cdot||} \mathbb{R}_{>0}) = \mathbb{I}_K^1/K^*.
\end{aligned}$$

Fact: We have a split short exact sequence:

$$0 \to C_K^1 \to C_K \to \mathbb{R}_{>0} \to 0.$$

This implies that $C_K \simeq C_K^1 \times \mathbb{R}_{>0}$.

Furthermore, we have proved that C_K^1 is compact last time.

5.1 The identity component of C_K

Definition 5.1. Let G be a topological group.

(1) $G^0 :=$ the identity component (i.e., the connected component of G containing e).
Fact: $G^0 \lhd G$.

(2) $g \in G$ is called **divisible** if $\forall n \in \mathbb{Z}_{\geq 1}$, $\exists h \in G$ s.t. $g = h^n$.

Remark:

(1) G is totally disconnected $\iff$ $G^0 = \{e\}$.

(2) In a finite group, the only divisible element is e. In a profinite group we have the same result.

(3) $\pi_0(G) := G/G^0$ is totally disconnected.

Exercise 5.1. H is a closed subgroup of G. If G/H is totally disconnected, then $H \supseteq G^0$.

Goal: Study C_K^0.

$$\mathbb{I}_K^0 = \prod_{v|\infty} (K_v^*)^0 \times \prod_{v\nmid\infty} \{1\},$$

$$\text{where } (K_v^*)^0 = \begin{cases} \mathbb{R}_{>0} & K_v = \mathbb{R} \\ \mathbb{C}^* & K_v = \mathbb{C} \end{cases}$$

Restrict the quotient map $\mathbb{I}_K \to C_K$ on $\mathbb{I}_K^0$. We have a map:

$\mathbb{I}_K^0 \to C_K^0$ (The image is contained in C_K^0 is because connected sets are mapped to connected sets).

Let D_K be the closure of the image of the composition map $\mathbb{I}_K^0 \hookrightarrow \mathbb{I}_K \to C_K$. Then $D_K \subseteq C_K^0$. **Fact:** This is an equality. We will prove it.

Proposition 5.1. $D_K = C_K^0 = \{\text{divisable elements in } C_K\}$. And C_K/D_K is profinite.

Remark: (GCFT) The Artin map $\psi_K : C_K \to \mathrm{Gal}(K^{ab}/K)$ has $\mathrm{Ker}(\psi_K) = D_K$. This is why we study D_K. It implies $C_K/D_K \simeq \mathrm{Gal}(K^{ab}/K)$.

Proof. We first show that C_K/D_K is profinite. (If this is proved, then by **Exercise 5.1**, $D_K \supseteq C_K^0$. This implies $D_K = C_K^0$).

To show C_K/D_K is profinite, we need to show:

(1) C_K/D_K is Hausdorff. (This is true since D_K is closed).

(2) C_K/D_K is compact.

Claim: The natural map $C_K^1 \hookrightarrow C_K \to C_K/D_K$ is a continuous surjection. If this is true, then since C_K^1 is compact, C_K/D_K is compact.

The claim can be easily proved. **Idea:** $C_K \simeq C_K^1 \times \mathbb{R}_{>0}$. The $\mathbb{R}_{>0}$ part is contained in D_K.

(3) C_K/D_K is totally disconnected.

We will use the following exercise:

Exercise 5.2. Let $\phi : G \to H$ be a surjective continuous homomorphism from a profinite group G to a Hausdorff topological group H. Then ϕ is a quotient map and H is profinite.

Let $U := \prod_{v|\infty} K_v^* \times \prod_{v\nmid\infty} \mathcal{O}_{K_v}^* \subset \mathbb{I}_K$. Let $\widetilde{U}$ be the image of U in C_K/D_K via the quotient map $\pi : \mathbb{I}_K \to C_K$. Since U is open in $\mathbb{I}_K$, $\widetilde{U}$ is open in C_K/D_K.

The map $U \to C_K/D_K$ will factor through $U' := \prod_{v \text{ real}}\{\pm 1\} \times \prod_{v \text{ complex}}\{1\} \times \prod_{v\nmid\infty} \mathcal{O}_{K_v}^*$. U' is totally disconnected. By **Exercise 5.2**, the continuous image $\widetilde{U}$ is also totally disconnected.

Since $\widetilde{U}$ is an open subgroup of C_K/D_K, it is also closed (clopen). The intersection $\widetilde{U} \cap (C_K/D_K)^0$ is a clopen subset of the connected space $(C_K/D_K)^0$. Since it contains the identity, it must be the whole space.

$$\implies (C_K/D_K)^0 \subseteq \widetilde{U}$$

Since $\widetilde{U}$ is totally disconnected, its only connected non-empty subspace is a point.

$$\implies (C_K/D_K)^0 = \{e\}$$
$$\implies C_K/D_K \text{ is totally disconnected.} \quad \square$$

Now we show that $D_K = \{\text{divisable elements in } C_K\}$.

($\supseteq$) Let d be a divisible element in C_K. Then its image $\bar{d}$ in C_K/D_K is also divisible. Since C_K/D_K is profinite, the only divisible element in it is the identity e. Thus $\bar{d} = e$, which means $d \in D_K$.

($\subseteq$) It suffices to show that for any $n \in \mathbb{N}^*$, the image of the map $\phi_n : C_K \to C_K$, $x \mapsto x^n$, contains D_K.

Recall: D_K is the closure of the image of the map $\prod_{v|\infty}(K_v^*)^0 \to C_K$.

The groups $(K_v^*)^0$ (which are $\mathbb{R}_{>0}$ or $\mathbb{C}^*$) are divisible. Therefore, the image of $\prod_{v|\infty}(K_v^*)^0$ in C_K is contained in the image of ϕ_n.

It remains to show that the subgroup $\mathrm{Im}(\phi_n)$ is closed in C_K. If it is, then it contains the closure of $\mathrm{Im}(\prod_{v|\infty}(K_v^*)^0)$, which is D_K.

To show that the image of the map $x \mapsto x^n$ is closed, we consider the isomorphism

$C_K \simeq C_K^1 \times \mathbb{R}_{>0}$. The map acts on each component.

$$\begin{array}{ccc} C_K & \simeq & C_K^1 \times \mathbb{R}_{>0} \\ \downarrow {\scriptstyle x \mapsto x^n} & \downarrow & \downarrow \\ C_K & \simeq & C_K^1 \times \mathbb{R}_{>0} \end{array}$$

Since C_K^1 is compact, the image of the map $x \mapsto x^n$ on C_K^1 is a compact and therefore closed subgroup. The map $x \mapsto x^n$ on $\mathbb{R}_{>0}$ is a homeomorphism, so the image is all of $\mathbb{R}_{>0}$. Thus, the image of the map on C_K is closed.

□

Remark: If there is only one Archimedean place (i.e., $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-d})$ is a quadratic imaginary field), then $D_K = (K_\infty^*)^0$.

- For $K = \mathbb{Q}$, $C_K^0 = \mathbb{R}_{>0}$.
- For $K = \mathbb{Q}(\sqrt{-d})$, $C_K^0 = \mathbb{C}^* \simeq \mathbb{R}_{>0} \times S^1$.

In general, the structure of the identity component C_K^0 is given by

$$C_K^0 \simeq \mathbb{R}_{>0} \times (S^1)^{r_2} \times (\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{r_1+r_2-1}$$

where r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings. The term $(\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{r_1+r_2-1}$ is related to a system of fundamental units $\epsilon_1^*, \ldots, \epsilon_{r_1+r_2-1}^*$.

The identity component of the norm-1 subgroup C_K^1 is then

$$(C_K^1)^0 \simeq (S^1)^{r_2} \times (\mathbb{A}_\mathbb{Q}/\mathbb{Q})^{r_1+r_2-1}$$

The group $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is the solenoid group. Reference: 3.3.

$$\mathbb{A}_\mathbb{Q}/\mathbb{Q} \simeq \mathbb{R} \times \hat{\mathbb{Z}}/\mathbb{Z} \simeq \varprojlim_n \mathbb{R}/n\mathbb{Z} \simeq \varprojlim_{x \mapsto x^n} S^1$$

The Solenoid (螺线管) is a compact and connected group.

II. Class Field Theory

5.2 Class Field Theory Over $\mathbb{Q}$

Recall: For $m \geq 1$, we have a canonical isomorphism for the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$:

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) &\simeq (\mathbb{Z}/m\mathbb{Z})^* \\ [\zeta_m \mapsto \zeta_m^a] &\longleftrightarrow \bar{a} \end{aligned}$$

A prime p is unramified in $\mathbb{Q}(\zeta_m) \iff p \nmid m$.

If $p \nmid m$, the Frobenius element is given by:

$$\mathrm{Frob}_p := \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) \longleftrightarrow \bar{p}.$$

This defines the Artin map for this extension:

$$\begin{aligned} \psi_m : (\mathbb{Z}/m\mathbb{Z})^* &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ \bar{a} &\mapsto \bar{a}^{-1} \end{aligned}$$

In particular for prime $p \nmid m$, $\psi_m(\bar{p}^{-1}) = \mathrm{Frob}_p$.

For $m|m'$, the following diagram commutes:

$$\begin{array}{ccc} (\mathbb{Z}/m'\mathbb{Z})^* & \xrightarrow{\psi_{m'}} & \mathrm{Gal}(\mathbb{Q}(\zeta_{m'})/\mathbb{Q}) \\ \downarrow & & \downarrow \\ (\mathbb{Z}/m\mathbb{Z})^* & \xrightarrow{\psi_m} & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \end{array}$$

Taking the inverse limit, we get an isomorphism:

$$\psi : \varprojlim_m (\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cycl}}/\mathbb{Q}).$$

The LHS is $\hat{\mathbb{Z}}^*$, and $\mathbb{Q}^{\mathrm{cycl}} = \bigcup_m \mathbb{Q}(\zeta_m)$.

Theorem 5.1 (**Kronecker-Weber**)**.** The maximal abelian extension of $\mathbb{Q}$ is the maximal cyclotomic extension:

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cycl}}.$$

This implies that the map ψ gives an isomorphism:

$$\psi : \hat{\mathbb{Z}}^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

We have the idele class group for $\mathbb{Q}$:

$$C_{\mathbb{Q}} = \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^*.$$
$$C^0_{\mathbb{Q}} = \mathbb{R}_{>0}.$$

The global Artin map for $\mathbb{Q}$ is given by:

$$\psi : C_{\mathbb{Q}}/C^0_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}).$$

Recall: For a finite abelian extension $K/\mathbb{Q}$, let p be a prime in $\mathbb{Q}$. The prime factorization in O_K is $pO_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_g^e$. We have $[K : \mathbb{Q}] = efg$. The decomposition group is $D(K|p) := D(\mathfrak{p}_i|p)$. The inertia group is $I(K|p) := I(\mathfrak{p}_i|p)$. We have a short exact sequence:

$$1 \to I(\mathfrak{p}_i|p) \to D(\mathfrak{p}_i|p) \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p}_i)/(\mathbb{Z}/p\mathbb{Z})) \to 1.$$

The orders of the groups are $|I| = e$ and $|D| = ef$. If p is unramified in K, then $I(K|p) = \{e\}$ and $D(K|p) = \langle \mathrm{Frob}_p \rangle$.

Example 5.1. Let $K_m = \mathbb{Q}(\zeta_m)$, with $m = p^r n$ and $p \nmid n$. The Galois group is

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

The subextension $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ is totally ramified at p. The subextension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is unramified at p. The inertia group of p in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is

$$I(\mathbb{Q}(\zeta_m)/\mathbb{Q}, p) = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_n)) \simeq (\mathbb{Z}/p^r\mathbb{Z})^*.$$

The decomposition group of p in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is

$$D(\mathbb{Q}(\zeta_m)/\mathbb{Q}, p) \simeq (\mathbb{Z}/p^r\mathbb{Z})^* \times \langle \bar{p} \rangle,$$

where $\bar{p}$ is the image of p in $(\mathbb{Z}/n\mathbb{Z})^*$.

Remark: Let $K \subset \mathbb{Q}(\zeta_m)$. If a prime p is unramified in K, then $K \subset \mathbb{Q}(\zeta_n)$, where $m = p^r n$ and $p \nmid n$.

Fact: Let $L/K/\mathbb{Q}$ be a tower of abelian extensions. The natural projection $\pi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ maps the decomposition and inertia groups of a prime p onto each other.

$$\pi(D(L|p)) = D(K|p)$$
$$\pi(I(L|p)) = I(K|p)$$

If p is unramified in L, then the Frobenius elements are also compatible:

$$\pi\left(\left(\frac{L/\mathbb{Q}}{p}\right)\right) = \left(\frac{K/\mathbb{Q}}{p}\right).$$

Corollary 5.1. Let $K/\mathbb{Q}$ be a finite abelian extension. The Artin map for this extension, $\psi_{K/\mathbb{Q}}$, is obtained by composing the global Artin map for $\mathbb{Q}$ with the natural projection:

$$\psi_{K/\mathbb{Q}} : C_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}}/C_{\mathbb{Q}}^0 \xrightarrow{\psi:\text{Kronecker-Weber}} \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

For any prime p, let $\mathbb{Q}_p^*$ and its subgroup of units $\mathbb{Z}_p^*$ be embedded in $C_{\mathbb{Q}}$ as the ideles which are 1 away from the place p. Then

$$\psi_{K/\mathbb{Q}}(\mathbb{Q}_p^*) = D(K|p)$$
$$\psi_{K/\mathbb{Q}}(\mathbb{Z}_p^*) = I(K|p)$$

Moreover, if p is unramified in K, then the idele corresponding to the local uniformizer $p \in \mathbb{Q}_p^*$ is mapped to the Frobenius element:

$$\psi_{K/\mathbb{Q}}(p) = \mathrm{Frob}_p.$$

Proof. By the Kronecker-Weber theorem and the compatibility of the Artin map, it is sufficient to prove this for a cyclotomic extension $K = K_m = \mathbb{Q}(\zeta_m)$. Let $m = p^r n$ with $p \nmid n$. We have the composition of maps:

$$\mathbb{Q}_p^* \hookrightarrow C_{\mathbb{Q}} \simeq \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^* \xrightarrow{\psi_{K_m/\mathbb{Q}}} (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

An element $a \in \mathbb{Z}_p^*$ is embedded into $\hat{\mathbb{Z}}^*$ as an element $(1, ..., 1, a, 1, ...)$ where a is at the p-th component. Under the projection map $\hat{\mathbb{Z}}^* \to (\mathbb{Z}/m\mathbb{Z})^*$, this maps to $(a^{-1} \pmod{p^r}, 1)$. The subgroup of such elements is $(\mathbb{Z}/p^r\mathbb{Z})^* \times \{1\}$, which is precisely the inertia group $I(K_m|p)$.

The prime p, as a local uniformizer in $\mathbb{Q}_p^*$, corresponds to the idele $(..., 1, p, 1, ...)$. By

quotienting out by $C_{\mathbb{Q}}^0 = \mathbb{R}_{>0}$, we can assume it corresponds to $(..., p^{-1}, 1, p^{-1}, ...)$ in $\hat{\mathbb{Z}}^*$. Its image under the map $\psi_{K_m/\mathbb{Q}}$ corresponds to $(1, \bar{p})$ in $(\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, which is the Frobenius element Frob_p.

Since $\mathbb{Q}_p^* = \langle p \rangle \times \mathbb{Z}_p^*$, its image under $\psi_{K_m/\mathbb{Q}}$ is generated by the images of p and $\mathbb{Z}_p^*$, which is $\langle (1, \bar{p}) \rangle \times ((\mathbb{Z}/p^r\mathbb{Z})^* \times \{1\})$. This is the decomposition group $D(K_m|p)$. □

5.3 Class Field Theory over $\mathbb{Q}_p$

Recall: Let L/K be a Galois extension of number fields. Let $v \in V_{K,f}$ be a finite place of K corresponding to a prime ideal $\mathfrak{p}_v$. Let w be a place of L lying above v, corresponding to a prime ideal $\mathfrak{P}_w$.

- The extension of completions L_w/K_v is a Galois extension of local fields.
- The local Galois group is isomorphic to the decomposition group of the global extension:

$$\mathrm{Gal}(L_w/K_v) \simeq D(\mathfrak{P}_w|\mathfrak{p}_v) \subseteq \mathrm{Gal}(L/K).$$

- The place v is unramified in $L \iff$ the local extension L_w/K_v is unramified $\iff$ $e = 1$.
- The local and global ramification indices and residue degrees are equal:

$$e(\mathfrak{P}_w|\mathfrak{p}_v) = e(L_w|K_v)$$
$$f(\mathfrak{P}_w|\mathfrak{p}_v) = f(L_w|K_v)$$

Example 5.2. Consider the local cyclotomic extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$. Let $m = p^r n$ with $p \nmid n$.

- The extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified $\iff p \nmid m$.
- The Galois group of the local extension is isomorphic to the decomposition group of the global extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ at p:

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) &\simeq D(\mathbb{Q}(\zeta_m)/\mathbb{Q}, p) \\ &\simeq (\mathbb{Z}/p^r\mathbb{Z})^* \times \langle \bar{p} \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^* \\ &\subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*\end{aligned}$$

- The inertia group of the local extension is

$$I(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) := \{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \mid \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in \mathcal{O}_{\mathbb{Q}_p(\zeta_m)}\}$$
$$\simeq I(\mathbb{Q}(\zeta_m)/\mathbb{Q}, p) \simeq (\mathbb{Z}/p^r\mathbb{Z})^*.$$

We have the short exact sequence for the local Galois group of $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$:

$$1 \to I(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \to 1$$

which corresponds to the group-theoretic sequence

$$1 \to (\mathbb{Z}/p^r\mathbb{Z})^* \to (\mathbb{Z}/p^r\mathbb{Z})^* \times \langle \bar{p} \rangle \to \langle \bar{p} \rangle \to 1$$

Taking the inverse limit over all m, we get a short exact sequence for the maximal cyclotomic extension of $\mathbb{Q}_p$:

$$\varprojlim_m : 1 \to I(\mathbb{Q}_p^{\mathrm{cycl}}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{cycl}}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to 1$$

The corresponding groups in the limit give the sequence:

$$1 \to \mathbb{Z}_p^* \to \mathbb{Z}_p^* \times \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \to 1$$

where $\mathbb{Q}_p^{\mathrm{cycl}} = \bigcup_{m \geq 1} \mathbb{Q}_p(\zeta_m)$.

Theorem 5.2 (**Local Kronecker-Weber**)**.** The maximal abelian extension of $\mathbb{Q}_p$ is the maximal cyclotomic extension:

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{cycl}}.$$

This implies there is an isomorphism:

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \simeq \mathbb{Z}_p^* \times \hat{\mathbb{Z}}.$$

The local Artin map is defined via the following commutative diagram, which connects the global and local theories.

$$\begin{array}{ccccc} C_{\mathbb{Q}} & \xrightarrow{\psi} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) & \to & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{Q}_p^* & \xrightarrow{\psi_p} & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) & \to & \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \end{array}$$

The vertical maps are the natural (of ideles on the left, and of decomposition groups on the right).

Definition 5.2. The **local Artin map** $\psi_p : \mathbb{Q}_p^* \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ is the unique map that makes the above diagram commute.

Corollary 5.2 (**Local-Global Compatibility**)**.** The local and global Artin maps for $\mathbb{Q}$ are compatible in the sense that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Q}_p^* & \xrightarrow{\psi_p} & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ C_{\mathbb{Q}} & \xrightarrow{\psi} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \end{array}$$

where the left vertical arrow is the canonical inclusion of the local field into the ideles, and the right vertical arrow is the inclusion of the decomposition group at p into the full Galois group.

Corollary 5.3. There is commutative diagram:

$$\begin{array}{ccc} \mathbb{Q}_p^* & \xrightarrow{\psi_p} & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \\ \downarrow{\scriptstyle \mathrm{order}} & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \simeq \hat{\mathbb{Z}} \end{array}$$

where $\mathbb{Q}_p^{\mathrm{ur}}$ is the maximal unramified extension of $\mathbb{Q}_p$.

Proof Sketch. It suffices to show that the composition

$$\mathbb{Q}_p^* \xrightarrow{\psi_p} \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \simeq \hat{\mathbb{Z}}$$

maps the subgroup of units $\mathbb{Z}_p^*$ to 0 and the uniformizer p to 1. This follows from the fact that $\psi_p(\mathbb{Z}_p^*)$ is the inertia group, which is the kernel of the projection onto the unramified quotient. □

5.4 Statements of Global Class Field Theory

Remark: In this part we will state the main theorems of global class field theory without proofs.

Theorem 5.3 (**Reciprocity Law**)**.** For any number field K, there is a continuous homomorphism with dense image,

$$\psi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

called the **global Artin map**, satisfying the following properties: For each finite abelian extension L/K, write the map $\psi_{L/K}$ is obtained by composing the global Artin map with the natural projection:

$$\psi_{L/K} : C_K \xrightarrow{\psi_K} \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K).$$

This map has the following properties:

1. $\psi_{L/K}$ is surjective with $\mathrm{Ker}(\psi_{L/K}) = N_{L/K}(C_L)$, where $N_{L/K}$ is the idele norm map. This induces an isomorphism $C_K/N_{L/K}(C_L) \simeq \mathrm{Gal}(L/K)$.

2. For each place $v \in V_K$, consider the composition (the local Artin map for L/K):

$$f_v : K_v^* \to C_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K).$$

   (2.1) If $v \in V_{K,f}$ (a finite place), then f_v kills the unit group $\mathcal{O}_{K_v}^*$ if and only if v is unramified in L. When this holds, f_v sends any uniformizer of K_v to the Frobenius element $\mathrm{Frob}_v \in \mathrm{Gal}(L/K)$.

   (2.2) If $v \in V_{K,\infty}$ (an infinite place), then f_v kills the identity component $(K_v^*)^0$.

   - When v is unramified in L, f_v is the trivial map.
   - When v is ramified in L (which implies $K_v \simeq \mathbb{R}$), f_v sends any negative number (e.g., -1) to the complex conjugation automorphism corresponding to v.

Definition 5.3. For an extension L/K and an infinite place $v \in V_{K,\infty}$, we say v is **unramified** in L if for every place w of L extending v, the local degree is $e(L_w|K_v) = 1$. Otherwise, we say v is **ramified**.

Remark: If $K_v \simeq \mathbb{C}$, then v is always unramified in L. Ramification at infinity can only occur for real places.

Theorem 5.4 (**Existence Theorem**)**.** A subgroup of C_K is an open subgroup of finite index if and only if it is of the form $N_{L/K}(C_L)$ for some finite abelian extension L/K.

Corollary 5.4. The global Artin map $\psi_K : C_K \to \mathrm{Gal}(K^{ab}/K)$ is surjective, and its kernel is the identity component of the idele class group, $\mathrm{Ker}(\psi_K) = D_K (= C_K^0)$. It induces a topological isomorphism:

$$C_K/D_K \simeq \mathrm{Gal}(K^{ab}/K).$$

Proof of the Corollary. We know that $D_K \subseteq \mathrm{Ker}(\psi_K)$ because D_K (being the identity component C_K^0) is connected, while the target group $\mathrm{Gal}(K^{ab}/K)$ is profinite and thus totally disconnected. The continuous image of a connected space must be connected, so $\psi_K(D_K)$ must be the identity element.

This implies that ψ_K factors through the quotient group:

$$C_K/D_K \to \mathrm{Gal}(K^{ab}/K).$$

This is a continuous homomorphism. It remains to show:

1. ψ_K is surjective.
2. $\mathrm{Ker}(\psi_K) \subseteq D_K$.

1. **Surjectivity:** By the Reciprocity Law, the image $\psi_K(C_K)$ is a dense subgroup of $\mathrm{Gal}(K^{ab}/K)$. The quotient group C_K/D_K is compact (**Proposition 5.1**). Since the map $C_K/D_K \to \mathrm{Gal}(K^{ab}/K)$ is continuous, its image, which is $\psi_K(C_K)$, is a compact subgroup. A subgroup of a Hausdorff topological group that is both dense and compact must be the entire group. Thus, $\psi_K(C_K) = \mathrm{Gal}(K^{ab}/K)$, and the map is surjective.

2. **Kernel:** The kernel of the global Artin map is the intersection of the kernels for all finite abelian extensions:

$$\begin{aligned}\mathrm{Ker}(\psi_K) &\subseteq \bigcap_{L/K \text{ fin. ab.}} \mathrm{Ker}(\psi_{L/K}) \\ &= \bigcap_{L/K \text{ fin. ab.}} N_{L/K}(C_L) \quad \text{(by the Reciprocity Law)}\end{aligned}$$

By the Existence Theorem, the set of norm groups $\{N_{L/K}(C_L)\}$ is precisely the set of all open subgroups of C_K of finite index. Therefore, $\mathrm{Ker}(\psi_K)$ is the intersection of all open subgroups of C_K of finite index.

So:

$$\begin{aligned}\mathrm{Ker}(\psi_K)/D_K &\subseteq \bigcap\{U/D_K | U \text{ open subgroup of } C_K \text{ containing } D_K \text{ with finite index } [C_K : U]\} \\ &= \bigcap\{U | U \text{ open subgroup of } C_K/D_K \text{ with finite index } [C_K/D_K : U]\}\end{aligned}$$

The group C_K/D_K is compact, so open subgroup is naturally of finite index. So:

$$\mathrm{Ker}(\psi_K)/D_K \subseteq \bigcap\{U | U \text{ open subgroup of } C_K/D_K\ \}$$

In a profinite group, the intersection of all open subgroups is the trivial subgroup. This means that the image of $\mathrm{Ker}(\psi_K)$ under the quotient map $C_K \to C_K/D_K$ is the trivial element. This implies that $\mathrm{Ker}(\psi_K) \subseteq D_K$.

□

5.5 Homework

Homework 5.1. Let $\phi : G \to H$ be a surjective continuous homomorphism from a profinite group G to a Hausdorff topological group H. Then ϕ is a quotient map and H is profinite.

Proof. • ϕ is closed map.

For any closed set $S \subseteq G$, G is profinite therefore compact, so S is compact. Since ϕ is continuous, $\phi(S)$ is compact. Since H is Hausdorff, $\phi(S)$ is closed.

- $V \subseteq H$ is open $\iff$ $\phi^{-1}(V)$ is open in G.

$\Rightarrow$ is true by continuity. For $\Leftarrow$, if V a set in H such that $\phi^{-1}(V)$ is open in G, then $G \setminus \phi^{-1}(V)$ is closed in G. Because ϕ is a surjective closed map, $H \setminus V = \phi(G \setminus \phi^{-1}(V))$ is closed in H, which implies V is open in H.

- ϕ is a quotient map.

For $G \xrightarrow{\pi} G/\ker\phi \xrightarrow{\psi} H$ such that $\psi \circ \pi = \phi$, π has the same two mentioned properties as ϕ for similar reasons. ψ is set and group theoretically bijective. For any $U \subseteq H$:

$$\begin{aligned} U \text{ is open in } H &\iff \phi^{-1}(U) \text{ is open in } G \\ &\iff \pi^{-1}(\psi^{-1}(U)) \text{ is open in } G \\ &\iff \psi^{-1}(U) \text{ is open in } G/\ker\phi \end{aligned}$$

Therefore, ϕ is a quotient map.

- H is compact.

G is profinite therefore compact, ϕ sends compact set to compact set, and ψ is surjective, so $H = \psi(G)$ is compact.

- ϕ is open map.

We only need to show the quotient map π is open. (Note: this is true for all topological groups.) For any open set $U \subseteq G$, we have:

$$\begin{aligned} \pi^{-1}(\pi(U)) &= \{g \in G | \exists u \in U, \text{ s.t. } gu^{-1} \in \ker\phi\} \\ &= \bigcup_{k \in \ker\phi} kU \quad \text{is open in } G. \end{aligned}$$

From the definition of quotient topology, $\pi(U)$ is open in $G/\ker\phi$.

- H is totally disconnected.

For any connected subset $S \subseteq H$ containing e_H, if there exists $h \in S \setminus \{e_H\}$. Because H is Hausdorff, $\{h\}$ is closed in H, so $e_G \in G \setminus \phi^{-1}(\{h\})$ is open in G.

Because G is profinite, well-known results say all open normal subgroup of G forms a basis of open neighborhood of e_G. So there exists an open normal subgroup $N \subseteq G$ such that $N \subseteq G \setminus \phi^{-1}(\{h\})$.

Also well-known results say N is also closed in G, so N is open in G. We have proved ϕ is open and closed map, therefore $\phi(N)$ is also clopen in H which dose not contain h. So:

$$S = (S \cap \phi(N)) \cup (S \cap \phi(N)^c)$$

separates e_H and h, so separates S into two non-empty disjoint open sets. Contradiction!

Therefore, $S = \{e_H\}$ and H is totally disconnected. □

Homework 5.2. G is a topological group, G^0 is the identity component.

(a) G/G^0 is totally disconnected.

(b) H is a closed subgroup of G. If G/H is totally disconnected, then $H \supseteq G^0$.

proof of (a). $\pi : G \to G/G^0$ is the quotient map.

- For any clopen set $U \subseteq G$, $g \in U$ if and only if $gG^0 \subseteq U$.

$\Leftarrow$ is trivial. For $\Rightarrow$, $g^{-1}U$ is a clopen set containing e_G, so $G^0 \subseteq g^{-1}U$, which implies $gG^0 \subseteq U$.

- For any clopen set $U \subseteq G$, $\pi(U) \cap \pi(U^c) = \emptyset$, so $\pi(U)$ is clopen in G/G^0.

If $\overline{g} \in \pi(U) \cap \pi(U^c)$ where $g \in G$, then there exists $g_1 \in U, g_2 \in U^c$ such that $gG^0 = g_1G^0 = g_2G^0$, then $gG^0 \subseteq U \cap U^c = \emptyset$, contradiction!

Quotient map is by definition an open map. So $\pi(U)$ is open in G/G^0, and at the same time $\pi(U) = G/G^0 \setminus \pi(U^c)$ is closed.

For any connected subset $S \subseteq G/G^0$, if there exists $\overline{g} \in S \setminus \{e_{G/G^0}\}$ where $g \in G \setminus G^0$, from the definition of G_0, there exists clopen $U \ni e_G$ such that $g \notin U$. So $U \cap gG^0 = \emptyset$ i.e. $\overline{g} \notin \pi(U)$. So from what we proved:

$$S = (S \cap \pi(U)) \cup (S \cap \pi(U^c))$$

is a disjoint union of open sets of S which separates e_{G/G^0} and $\overline{g}$, contradiction!

So $S = \{e_{G/G^0}\}$, G/G^0 is totally disconnected.

□

proof of (b). $\pi : G \to G/H$ is the quotient map. Continuous map sends connected set to connected set, so $\pi(G^0)$ is a connected set in G/H containing $e_{G/H}$. Since G/H is totally disconnected, $\pi(G^0) = \{e_{G/H}\}$, which implies $G^0 \subseteq H$. □

Homework 5.3. (a) For any $v \in V_K$, $K_v^* \to C_K$ is a closed embedding.

(b) If $S \subset V_K$ is a finite set of places and $|S| > 1$, then $\prod_{v\in S} K_v^* \to C_K$ is not a closed embedding.

proof of (a). $\varphi : K_v^* \xrightarrow{\iota} \mathbb{I}_K \xrightarrow{\pi} C_K$ factors through $\mathbb{I}_K$.

(*) For any closed subset $Z \subseteq K_v^*$, we have

$$\widetilde{Z} := \pi^{-1}\varphi(Z) = K^*\iota(Z) := \{(k, \ldots, k, ka, k, \ldots) | k \in K, a \in Z, ka \text{ is at the } v\text{-th place}\}$$

is closed in $\mathbb{I}_K$.

For any $y = (y_w)_w \notin \widetilde{Z}$,

- There are finitely many $k \in K$ such that
  - for all $w \in V_{K,f} \setminus \{v\}$, $|k|_w = |y_w|_w$.
  - for all $w \in V_{K,\infty} \setminus \{v\}$, $|k|_w \in [|y_w|_w/2, 2|y_w|_w]$.

By the product formula, for any k satisfying the above condition we can know $|k|_w$ for all $w \in V_K$. By multiplying k by some element k_0 in $\mathbb{Z}$ we can get $|k/k_0|_w \leqslant 1$. Now $k/k_0 \in \mathcal{O}_K$ and we know $|k/k_0|_w$ for all $w \in V_{K,\infty}$. So by Vieta, analyzing the absolute number of the coefficients, the choices of the minimal polynomial of k/k_0 are finite. Therefore, the choices of k are finite.

We collect all such k's into a finite set F.

If there exists $k \in K$ such that $k = y_w$ for all $w \neq v$, then $y_v \notin kZ$. Therefore, there exists an open neighborhood U_v of y_v in K_v^* such that $U_v \cap kZ = \emptyset$. Let $U = \prod_{w\neq v} \mathcal{O}_{K_w}^* \times U_v$, then U is an open neighborhood of y in $\mathbb{I}_K$ and $U \cap \widetilde{Z} = \emptyset$.

If there exists $k_1 \neq k_2$ and $w_1, w_2 \neq v$ such that $k_i = y_{w_i}$ for $i = 1, 2$, we can choose neighborhood $U_{w_i} \ni y_{w_i}$ such that $U_{w_i} \cap F = \emptyset$ and $|U_{w_i}|_{w_i} = |y_{w_i}|_{w_i}$. Let $U = \prod_{w\neq T} \mathcal{O}_{K_w}^* \times$

$U_{w_1} \times U_{w_2} \times \prod_{w \in T} U_w$, where T is the set of places $w \neq v, w_1, w_2$ such that $|y_w|_w \neq 1$ and U_w is a small neighborhood of y_w. Then U is an open neighborhood of y in $\mathbb{I}_K$ and $U \cap \widetilde{Z} = \emptyset$.

If there is $w_0 \neq v$ such that $y_{w_0} \notin F$, we can choose a neighborhood $U_{w_0} \ni y_{w_0}$ such that $U_{w_0} \cap F = \emptyset$ and $|U_{w_0}|_{w_0} = |y_{w_0}|_{w_0}$. Similar way as above we can construct an open neighborhood U of y in $\mathbb{I}_K$ such that $U \cap \widetilde{Z} = \emptyset$.

Therefore, $\widetilde{Z}$ is closed in $\mathbb{I}_K$.

Combine (*) with the fact that φ is injective, we know φ is a closed embedding. □

proof of (b) for trivial case. **Remark:** I can only construct a counterexample when $K = \mathbb{Q}$. I think the general case is similar.

Let $S = \{\infty, 2\}$, our goal is to show

$$J := \pi^{-1}\phi(\prod_{v \in S} K_v^*) = \{(k, \ldots, k, k(a), k, \ldots) | k \in K, (a) \in \prod_{v \in S} K_v^*\}$$

is not closed in $\mathbb{I}_\mathbb{Q}$, where $\phi : \prod_{v \in S} K_v^* \to C_K$ and $\pi : \mathbb{I}_K \to C_K$ are the natural maps.

For $(y_p)_p \in \mathbb{I}_\mathbb{Q}$ to be choosed later, and its neighbourhood

$$U = V \times U_2 \times \prod_{p \in T} U_p \times \prod_{p \notin T \cup \{2, \infty\}} \mathbb{Z}_p^*$$

where V is a neighborhood of y_∞ in $\mathbb{R}^*$, T is a finite set of primes not containing 2, U_2, U_p are neighborhoods of y_2, y_p in $\mathbb{Q}_2^*, \mathbb{Q}_p^*$ respectively.

For $p \neq 2$, we choose $y_p \in \mathbb{Z}_p$ such that:

$$y_p \equiv 2^{r_p + \varphi(p^2) + \ldots + \varphi(p^{n-1})} := y_p^{(n)} \pmod{p^n},\ \forall n \geqslant 1$$

Or in another word, y_p is the limit of the sequence $\{2^{r_p + \varphi(p^2) + \ldots + \varphi(p^{n-1})}\}_{n \geqslant 1}$ in $\mathbb{Z}_p$, where r_p is still to be determined.

Our goal is that: for any $m \in \mathbb{N}$, we want to find $l_m \in \mathbb{N}$ such that

$$2^{l_m} \equiv y_p^{(m)} \pmod{p^m},\ \forall p \in T$$

If we can do this, then for any neighbourhood U defined above, we can find m large enough such that $y_p^{(m)} \in U_p$ for all $p \in T$, and then we can find l_m such that $(*, 2^{l_m}, 2^{l_m}, 2^{l_m}, \ldots) \in U \cap J$, which implies J is dense in U, while $(y_p)_p$ we constructed is in U but not in J.

It is sufficient to solving the following system of congruences:

$$l_m \equiv r_p + \varphi(p^2) + \ldots + \varphi(p^{m-1}) \pmod{\varphi(p^m)},\ \forall p \in T$$

So we can construct r_p inductively to make the system solvable. In detail: If $r_3, \ldots, r_p$ are already constructed, for the next prime q, we can choose r_q such that

$$r_q \equiv r_p + \varphi(p^2) + \ldots + \varphi(p^{m-1}) \pmod{q-1}, \quad \forall p^m || q-1$$

We now have done the construction. □

proof of (b) for general case. **Remark:** Express my sincere thanks to Xiaobo Feng.

Firstly we state three lemmas.

Lemma 5.1. $\Gamma \subseteq \mathbb{R}^n$ is a free $\mathbb{Z}$-module of rank $m > n$, then in the Euclidean topology,

$$|\mathrm{cl}_{\mathbb{R}^n}(\Gamma)| = \aleph$$

proof of Lemma 5.1. Γ has a $\mathbb{Z}$-basis $\{v_1, \ldots, v_m\}$. We can choose the maximal $\mathbb{R}$-linearly independent subset (without loss of generality) $\{v_1, \ldots, v_r\}$ of $\{v_1, \ldots, v_m\}$. Because $m > n \geqslant r$, $\{v_1, \ldots, v_{r+1}\}$ can form a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module $\Gamma' \subseteq \mathbb{R}v_1 \oplus \ldots \oplus \mathbb{R}v_r$ of rank $r+1$, which can't be discrete in $\mathbb{R}v_1 \oplus \ldots \oplus \mathbb{R}v_r$.

Suppose $v_{r+1} = a_1v_1 + \ldots + a_rv_r$ for some unique $a_i \in \mathbb{R}$. There exists (without loss of generality) $a_1 \in \mathbb{R} \setminus \mathbb{Q}$. For any $a \in \mathbb{R}$, we can find a sequence $\{c_k\}_{k\geqslant 1} \subseteq \mathbb{Z}$ such that:

$$\lim_{k\to\infty} \{c_k a_1\} = \{a\}$$

Note that:

$$\left\{\{c_k a_1\}v_1 + \{c_k a_2\}v_2 + \ldots + \{c_k a_r\}v_r\right\}_{k\geqslant 1} \subseteq \left\{s_1v_1 + s_2v_2 + \ldots + s_rv_r | s_i \in [0,1]\right\}$$

also LHS$\subseteq \Gamma'$, RHS is compact, so there exists a convergent subsequence of Γ', which converges to some v. Then v must have the form:

$$v = av_1 + *v_2 + \ldots + *v_r$$

So the closure of Γ' contains uncountably many elements. □

Lemma 5.2. Let $K_v/\mathbb{Q}_p$ be a finite local field extension. Let π_v be a uniformizer of K_v and $p = \pi_v^e$. Then for $n > \frac{e}{p-1}$, the power series:

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$
$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \ldots$$

form a homeomorphism between:

$$(\pi_v^n \mathcal{O}_{K_v}, +) \leftrightarrow (1 + \pi_v^n \mathcal{O}_{K_v}, \cdot)$$

The Lemma 5.2 is obtained from Neukirch's *Algebraic Number Theory, Chapter II, §5,*

Proposition 5.5.

Lemma 5.3. For $v \in V_{K,f}$, if $\xi \in \mathcal{O}_{K_v}^*$ and $\#\xi^{\mathbb{Z}} = +\infty$, then:

$$|\mathrm{cl}_{K_v^*}(\xi^{\mathbb{Z}})| \geqslant \aleph$$

proof of Lemma 5.3. Without loss of generality, we may assume $\xi \in 1 + \pi_v \mathcal{O}_{K_v}$, otherwise we know $f = |\mathcal{O}_{K_v}/\pi_v\mathcal{O}_{K_v}|$ is finite, then $\xi^f \in 1 + \pi_v\mathcal{O}_{K_v}$ and to prove $|\mathrm{cl}_{K_v^*}(\xi^{f\mathbb{Z}})| \geqslant \aleph$.

Suppose $K_v/\mathbb{Q}_p$ is the local field extension with ramification index e. $\#\xi^{p^2\mathbb{Z}}$ must be infinite, otherwise ξ is a root of unity which contradicts the assumption. Obviouly for sufficiently large n,

$$\mathrm{cl}_{K_v^*}(\xi^{\mathbb{Z}}) \supseteq \mathrm{cl}_{K_v^*}(\xi^{p^n\mathbb{Z}}) \supseteq \mathrm{cl}_{1+\pi_v^{ne}\mathcal{O}_{K_v}}(\xi^{p^n\mathbb{Z}})$$

and simultaneously $\xi^{p^n\mathbb{Z}} \subseteq 1 + \pi_v^{ne}\mathcal{O}_{K_v}$.

By **Lemma 5.2**,

$$|\mathrm{cl}_{1+\pi_v^{ne}\mathcal{O}_{K_v}}(\xi^{p^n\mathbb{Z}})| = |\mathrm{cl}_{\pi_v^{ne}\mathcal{O}_{K_v}}(p^n\mathbb{Z}\log(\xi))| \geqslant |p^n\mathbb{Z}_p\log(\xi)| = |p^n\mathbb{Z}_p| = \aleph$$

(Remark: $|p^n\mathbb{Z}_p\log(\xi)| = |p^n\mathbb{Z}_p|$ needs log is homeomorphism and hence injective on $1 + \pi_v^{ne}\mathcal{O}_{K_v}$.) Above all imply the lemma. □

Now we back to prove the general case of (b). Recall:

$$\begin{aligned} &\varphi : \prod_{v\in S} K_v^* \xrightarrow{\iota} \mathbb{I}_K \xrightarrow{\pi} C_K \text{ is not closed embedding} \\ \Longleftrightarrow &K^* \cdot \iota\left(\prod_{v\in S} K_v^*\right) \text{ is not closed in } \mathbb{I}_K \end{aligned}$$

So our main goal is to find $(y_v)_v \in \mathbb{I}_K \setminus K^* \cdot \iota\left(\prod_{v\in S} K_v^*\right)$ such that for any neighborhood U of $(y_v)_v$ in $\mathbb{I}_K$, we have:

$$U \cap K^* \cdot \iota\left(\prod_{v\in S} K_v^*\right) \neq \emptyset$$

1. $S \cap V_{K,\infty} = \emptyset$**, hence** $S \cap V_{K,f}$ **has at least two elements.**

We assume $v_1, v_2 \in S \cap V_{K,f}$ respectively corresponding to primes $\mathfrak{p}_1, \mathfrak{p}_2$. We know that the class number $\mathrm{Cl}(K)$ is finite, so $\mathfrak{p}_1^{\mathrm{Cl}(K)}, \mathfrak{p}_2^{\mathrm{Cl}(K)}$ must both be principal, respectively

$(\eta_1), (\eta_2)$. This means that for $v \in V_{K,f}$, $i = 1, 2$

$$\mathrm{ord}_v(\eta_i) \neq 0 \iff v = v_i \quad \text{and} \quad \mathrm{ord}_{v_i}(\eta_i) > 0$$

Consider the natural map:

$$\begin{aligned} K^* &\xrightarrow{\Phi} \mathbb{R}^{r_1+r_2} \\ x &\mapsto (\log |x|_v)_{v \in V_{K,\infty}} \end{aligned}$$

We **claim** that $\Phi(\eta_1), \Phi(\eta_2), \Phi(\mathcal{O}_K^*)$ are $\mathbb{Z}$-linearly independent in $\mathbb{R}^{r_1+r_2}$.

If $n_1, n_2 \in \mathbb{Z}$ and $\beta \in \mathcal{O}_K^*$ such that for all $v \in V_{K,\infty}$, $|\eta_1^{n_1}\eta_2^{n_2}\beta|_v = 1$, then $\eta_1^{n_1}\eta_2^{n_2}\beta \in (\mathcal{O}_K^*)^{\mathrm{tor}} \subseteq \mathcal{O}_K^*$. By taking ord_{v_i} on both sides for $i = 1, 2$, we get $n_1 = n_2 = 0$, so $\beta \in (\mathcal{O}_K^*)^{\mathrm{tor}}$ hence $\Phi(\beta) = 0$. This proves the claim.

By the Dirichlet's Unit Theorem and the claim, $\Phi(\eta_1^{\mathbb{Z}}\eta_2^{\mathbb{Z}}\mathcal{O}_K^*)$ is a free $\mathbb{Z}$-module of rank $r_1 + r_2 + 1$ in $\mathbb{R}^{r_1+r_2}$. By **Lemma 5.1**,

$$|\mathrm{cl}_{\mathbb{R}^{r_1+r_2}}\Phi(\eta_1^{\mathbb{Z}}\eta_2^{\mathbb{Z}}\mathcal{O}_K^*)| = \aleph > |\Phi(K^*)| = \aleph_0$$

So there exists $(t_v)_{v \in V_{K,\infty}} \in \mathbb{R}^{r_1+r_2} \setminus \Phi(K^*)$, and a sequence $\{x_n\}_{n \geqslant 1} \subseteq \eta_1^{\mathbb{Z}}\eta_2^{\mathbb{Z}}\mathcal{O}_K^*$ such that

$$\lim_{n \to \infty} \Phi(x_n) = (t_v)_{v \in V_{K,\infty}}$$

Because of the compactness of $\{\pm 1\}^{r_1} \times (S^1)^{r_2}$, the sequence

$$\{(|x_n|_v)_{v \in V_{K,\infty}}\}_{n \geqslant 1} \subseteq \prod_{v \in V_{K,\infty}} K_v^*$$

has a convergent subsequence, without loss of generality we still denote it by $\{(|x_n|_v)_v\}_{n \geqslant 1}$. Suppose there exists $k \in K^*$ such that for all $v \in V_{K,\infty}$,

$$\lim_{n \to \infty} (|x_n|_v)_v = (|k|_v)_v$$

Then for all $v \in V_{K,\infty}$, $t_v = \log(|k|_v)$, which contradicts the choice of $(t_v)_v \in \mathbb{R}^{r_1+r_2} \setminus \Phi(K^*)$.

Note that for all $v \in V_{K,f} \setminus S$,

$$\eta_1^{\mathbb{Z}}\eta_2^{\mathbb{Z}}\mathcal{O}_K^* \subseteq \mathcal{O}_{K_v}^*$$

Because of the compactness of $\prod_{v\in V_{K,f}\setminus S}\mathcal{O}_{K_v}^*$, for the sequence

$$\{x_n\cdot(1)_{v\in V_{K,f}\setminus S}\}_{n\geqslant 1}\subseteq\prod_{v\in V_{K,f}\setminus S}\mathcal{O}_{K_v}^*$$

there exists a convergent subsequence, without loss of generality we still denote it by $\{x_n\cdot(1)_{v\in V_{K,f}\setminus S}\}_{n\geqslant 1}$, converge to $(y_v)_{v\in V_{K,f}\setminus S}$.

Consider:

$$y=(y_v)_v=((t_v)_{v\in V_{K,\infty}},(y_v)_{v\in V_{K,f}\setminus S},(1)_{v\in S})\in\mathbb{I}_K$$

From the construction of $(t_v)_v$ and $(y_v)_{v\in V_{K,f}\setminus S}$, $y\notin K^*\cdot\iota\left(\prod_{v\in S}K_v^*\right)$. and for any neighborhood U of y in $\mathbb{I}_K$, there exists $N\in\mathbb{N}$ and $\alpha\in\iota(\prod_{v\in S}K_v^*)$ such that $x_N\alpha\in U$. Therefore we finish the proof in this case.

2. $|S\cap V_{K,\infty}|=1$ **and hence** $S\cap V_{K,f}\neq\emptyset$.

There is $v\in V_{K,f}\cap S$. In the similar way as above, there exists $\eta\in K^*$ such that for all $w\in V_{K,f}$,

$$\mathrm{ord}_w(\eta)\neq 0\iff w=v\quad\text{and}\quad\mathrm{ord}_v(\eta)>0$$

Consider the commutative diagram:

$$\begin{array}{ccccc}K^* & \xrightarrow{\rho} & \prod_{v\in V_{K,\infty}}K_v^* & \xrightarrow{\mathrm{pr}} & \prod_{v\in V_{K,\infty}\setminus S}K_v^*\\ & & \downarrow{\scriptstyle\log} & & \downarrow{\scriptstyle\log}\\ & & \mathbb{R}^{r_1+r_2} & \xrightarrow{\mathrm{pr}} & \mathbb{R}^{r_1+r_2-1}\end{array}$$

2.1. If $\mathrm{pr}\circ\log\circ\rho(\eta)=0$.

In this case, for all $v\in V_{K,\infty}\setminus S$, $|\eta|_v=1$.

We arbitrarily choose $v'\in V_{K,f}\setminus S$, Because η can't be a root of unity in K^*, $|\eta^{\mathbb{Z}}|=+\infty$. So by **Lemma 5.3**, there exists $s_{v'}\in\mathcal{O}_{K_{v'}}^*\setminus K^*$ and a subsequence

$$\{\eta^{l_n}\}_{n\in\mathbb{N}}$$

such that $\lim_{n\to\infty}\eta^{l_n}=s_{v'}$ in $K_{v'}^*$.

Because of the compactness of $\prod_{v\in V_{K,f}\setminus S}\mathcal{O}_{K_v}^*$, for the sequence

$$\{\eta^{l_n}\cdot(1)_{v\in V_{K,f}\setminus S}\}_{n\in\mathbb{N}}\subseteq\prod_{v\in V_{K,f}\setminus S}\mathcal{O}_{K_v}^*$$

there exists a convergent subsequence, without loss of generality we still denote it by $\{\eta^{l_n} \cdot (1)_{v\in V_{K,f}\setminus S}\}_{n\in\mathbb{N}}$. So the sequence satisfies:

- the sequence converges in $\prod_{v\in V_{K,f}\setminus S}\mathcal{O}_{K_v}^*$ to $(s_v)_{v\in V_{K,f}\setminus S}$
- $\lim_{n\to\infty}\eta^{l_n} = s_{v'}$ in $\mathcal{O}_{K_{v'}}^* \setminus K^*$.

Recall that in this case:

$$\{\eta^{l_n}\cdot(1)_{v\in V_{K,\infty}\setminus S}\}_{n\in\mathbb{Z}} \subseteq \underbrace{\{\pm 1\}\times\ldots\times\{\pm 1\}}_{|S\cap V_{K,\text{real}}|\text{ times}} \times \underbrace{S^1\times\ldots\times S^1}_{|S\cap V_{K,\text{complex}}|\text{ times}}$$

RHS is compact, so there exists a convergent subsequence, without loss of generality we still denote it by $\{\eta^{l_n}\cdot(1)_{v\in V_{K,\infty}\setminus S}\}_{n\in\mathbb{N}}$, converge to $(s_v)_{v\in V_{K,\infty}\setminus S}$.

Consider:

$$y = ((s_v)_{v\in V_{K,\infty}\setminus S}, (s_v)_{v\in V_{K,f}\setminus S}, (1)_{v\in S}) \in \mathbb{I}_K$$

Because $s_{v'}\notin K^*$, $y\notin K^*\cdot\iota\left(\prod_{v\in S}K_v^*\right)$. For any neighborhood U of y in $\mathbb{I}_K$, there exists $N\in\mathbb{N}$ and $\alpha\in\iota(\prod_{v\in S}K_v^*)$ such that $\eta^{l_N}\alpha\in U$. Therefore we finish the proof in this case.

2.2. If $\mathrm{pr}\circ\log\circ\rho(\eta)\neq 0$.

In this case, we note that:

$$\{X_1+X_2+\ldots+X_{r_1+r_2}=0\}\cap\ker(\mathrm{pr}) = \{0\}\subseteq\mathbb{R}^{r_1+r_2}$$

So by the Dirichlet's Unit Theorem, $\mathrm{pr}\circ\log\circ\rho(\mathcal{O}_K^*)$ is a full discrete lattice in $\mathbb{R}^{r_1+r_2-1}$ denoted by Λ.

(2.2.1) If $\Lambda+\mathbb{Z}\cdot(\mathrm{pr}\circ\log\circ\rho(\eta))$ is discrete.

Then there exists $\beta\in\mathcal{O}_K^*$ and $m\in\mathbb{Z}$ such that $\mathrm{pr}\circ\log\circ\rho(\beta^{-1}\eta^m)=0$. Consider the element $\beta^{-1}\eta^m$, we can reduce to the case (2.1).

(2.2.2) If $\Lambda+\mathbb{Z}\cdot(\mathrm{pr}\circ\log\circ\rho(\eta))$ is not discrete.

By **Lemma 5.1** and the similar argument as in case 1, there exists $(t_v)_{v\in V_{K,\infty}\setminus S}\in\prod_{v\in V_{K,\infty}\setminus S}K_v^*\setminus\mathrm{pr}\circ\rho(K^*)$, and a sequence $\{x_n\}_{n\geqslant 1}\subseteq\eta^{\mathbb{Z}}\mathcal{O}_K^*$ such that

$$\lim_{n\to\infty}\mathrm{pr}\circ\rho(x_n) = (t_v)_{v\in V_{K,\infty}\setminus S}$$

Still the similar argument as in case 1 shows that the sequence $\{x_n\}_{n\geqslant 1}$ has a convergent subsequence (WLOG still denoted by $\{x_n\}_{n\geqslant 1}$) such that:

$$\lim_{n\to\infty} x_n \cdot (1)_{v\in V_{K,f}\setminus S} = (t_v)_{v\in V_{K,f}\setminus S}$$

Consider

$$y = (y_v)_v = ((t_v)_{v\in V_{K,\infty}\setminus S}, (t_v)_{v\in V_{K,f}\setminus S}, (1)_{v\in S}) \in \mathbb{I}_K$$

From the construction of $(t_v)_{v\in V_{K,\infty}\setminus S}$, we have $y \notin K^* \cdot \iota\left(\prod_{v\in S} K_v^*\right)$. For any neighborhood U of y in $\mathbb{I}_K$, there exists $N \in \mathbb{N}$ and $\alpha \in \iota(\prod_{v\in S} K_v^*)$ such that $x_N\alpha \in U$. Therefore we finish the proof in this case.

3. $|S \cap V_{K,\infty}| \geqslant 2$**.**

Denote $r = |S \cap V_{K,\infty}| \geqslant 2$.

$$\begin{array}{ccccc} K^* & \xrightarrow{\rho} & \prod_{v\in V_{K,\infty}} K_v^* & \xrightarrow{\text{pr}} & \prod_{v\in V_{K,\infty}\setminus S} K_v^* \\ & & \downarrow{\scriptstyle \log} & & \downarrow{\scriptstyle \log} \\ & & \mathbb{R}^{r_1+r_2} & \xrightarrow{\text{pr}} & \mathbb{R}^{r_1+r_2-r} \end{array}$$

Denote $\Lambda := \log\circ\rho(\mathcal{O}_K^*) \subseteq H$ a discrete lattice of rank $r_1 + r_2 - 1$.

3.1. If $\Lambda \cap \mathrm{Ker}(\text{pr}) \neq \{0\}$.

Then there exists $\beta \in \mathcal{O}_K^* \setminus (\mathcal{O}_K^*)^{\text{tor}}$ such that $\text{pr}\circ\log\circ\rho(\beta) = 0$.

We arbitrarily choose $v' \in V_{K,f}\setminus S$, Because β can't be a root of unity in K^*, $|\beta^{\mathbb{Z}}| = +\infty$. So by **Lemma 5.3**, there exists $s_{v'} \in \mathcal{O}_{K_{v'}}^* \setminus K^*$ and a subsequence $\{\beta^{l_n}\}_{n\in\mathbb{N}}$ such that $\lim_{n\to\infty} \beta^{l_n} = s_{v'}$ in $K_{v'}^*$.

Because of the compactness of $\prod_{v\in V_{K,f}\setminus S} \mathcal{O}_{K_v}^*$, for the sequence

$$\{\beta^{l_n} \cdot (1)_{v\in V_{K,f}\setminus S}\}_{n\in\mathbb{N}} \subseteq \prod_{v\in V_{K,f}\setminus S} \mathcal{O}_{K_v}^*$$

there exists a convergent subsequence, without loss of generality we still denote it by $\{x_n \cdot (1)_{v\in V_{K,f}\setminus S}\}_{n\in\mathbb{N}}$. So the sequence satisfies:

- the sequence converges in $\prod_{v\in V_{K,f}\setminus S} \mathcal{O}_{K_v}^*$ to $(s_v)_{v\in V_{K,f}\setminus S}$
- $\lim_{n\to\infty} \beta^{l_n} = s_{v'}$ in $\mathcal{O}_{K_{v'}}^* \setminus K^*$.

Recall that in this case:

$$\{\beta^{l_n}\cdot(1)_{v\in V_{K,\infty}\setminus S}\}_{n\in\mathbb{Z}}\subseteq \underbrace{\{\pm1\}\times\ldots\times\{\pm1\}}_{|S\cap V_{K,\text{real}}|\text{ times}}\times\ \underbrace{S^1\times\ldots\times S^1}_{|S\cap V_{K,\text{complex}}|\text{ times}}$$

RHS is compact, so there exists a convergent subsequence, without loss of generality we still denote it by $\{\beta^{l_n}\cdot(1)_{v\in V_{K,\infty}\setminus S}\}_{n\in\mathbb{N}}$, converge to $(s_v)_{v\in V_{K,\infty}\setminus S}$.

Consider:

$$y=((s_v)_{v\in V_{K,\infty}\setminus S},(s_v)_{v\in V_{K,f}\setminus S},(1)_{v\in S})\in\mathbb{I}_K$$

Because $s_{v'}\notin K^*$, $y\notin K^*\cdot\iota\left(\prod_{v\in S}K_v^*\right)$. For any neighborhood U of y in $\mathbb{I}_K$, there exists $N\in\mathbb{N}$ and $\alpha\in\iota(\prod_{v\in S}K_v^*)$ such that $\beta^{l_N}\alpha\in U$. Therefore we finish the proof in this case.

3.2. If $\Lambda\cap\mathrm{Ker}(\mathrm{pr})=\{0\}$.

Then $\mathrm{pr}(\Lambda)$ is a free $\mathbb{Z}$-module of rank r_1+r_2-1 in $\mathbb{R}^{r_1+r_2-r}$.

By **Lemma 5.1** and the similar argument as in case 1, there exists $(t_v)_{v\in V_{K,\infty}\setminus S}\in\prod_{v\in V_{K,\infty}\setminus S}K_v^*\setminus\mathrm{pr}\circ\rho(K^*)$, and a sequence $\{x_n\}_{n\geqslant1}\subseteq\mathcal{O}_K^*$ such that

$$\lim_{n\to\infty}\mathrm{pr}\circ\rho(x_n)=(t_v)_{v\in V_{K,\infty}\setminus S}$$

Still the similar argument as in case 1 shows that the sequence $\{x_n\}_{n\geqslant1}$ has a convergent subsequence (WLOG still denoted by $\{x_n\}_{n\geqslant1}$) such that:

$$\lim_{n\to\infty}x_n\cdot(1)_{v\in V_{K,f}\setminus S}=(t_v)_{v\in V_{K,f}\setminus S}$$

Consider

$$y=(y_v)_v=((t_v)_{v\in V_{K,\infty}\setminus S},(t_v)_{v\in V_{K,f}\setminus S},(1)_{v\in S})\in\mathbb{I}_K$$

From the construction of $(t_v)_{v\in V_{K,\infty}\setminus S}$, we have $y\notin K^*\cdot\iota\left(\prod_{v\in S}K_v^*\right)$. For any neighborhood U of y in $\mathbb{I}_K$, there exists $N\in\mathbb{N}$ and $\alpha\in\iota(\prod_{v\in S}K_v^*)$ such that $x_N\alpha\in U$. Therefore we finish the proof in this case.

All in all, we have finished the proof of (b). □

Homework 5.4. Show that every open subgroup of C_K is of finite index.

Proof. For all open subgroup U of C_K, U is clopen in C_K, so $D_K \subseteq U$, and U/D_K is open in C_K/D_K. Since we have proved C_K/D_K is profinite (therefore compact), $[C_K/D_K : U/D_K] < \infty$. This implies $[C_K : U] < \infty$,

□

6 2025.10.16

Corollary 6.1 (**Classification of finite abelian extensions**)**.** The map

$$\{\text{finite abelian extensions of } K\} \longrightarrow \{\text{open subgroups of } C_K \text{ of finite index}\}$$
$$L \longmapsto N_{L/K}(C_L)$$

is bijective, inclusion reversing.

Proof. From Existence theorem, the map is well-defined and surjective. It remains to show $L \subseteq L' \Leftrightarrow N_{L'/K}(C_{L'}) \subseteq N_{L/K}(C_L)$.

"⇒": is obvious from $N_{L'/K} = N_{L/K} \circ N_{L'/L}$.

"⇐": Let $M = L \cdot L'$ is also an abelian extension of K. Consider the isomorphism:

$$C_K/N_{M/K}(C_M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

Then there are two correspondence:

$$N_{L/K}(C_L)/N_{M/K}(C_M) \longleftrightarrow \mathrm{Gal}(M/L)$$
$$N_{L'/K}(C_{L'})/N_{M/K}(C_M) \longleftrightarrow \mathrm{Gal}(M/L')$$

By assumption, $N_{L'/K}(C_{L'}) \subseteq N_{L/K}(C_L)$, so $\mathrm{Gal}(M/L) \subseteq \mathrm{Gal}(M/L')$, which implies $L \subseteq L'$. □

Proposition 6.1. The global Artin map is uniquely determined by **Theorem 5.3 (2.1)**. More precisely: L/K is a finite abelian extension, Let $\phi, \phi' : C_K \to \mathrm{Gal}(L/K)$ be continuous homomorphisms. Suppose there exists a finite set of places $S \subseteq V_K$, containing all archimedean places and all places that ramify in L, such that for all $v \in V_K \setminus S$, the following compositions are equal for every uniformizer of K_v^*:

$$K_v^* \xrightarrow{i_v} C_K \underset{\phi'}{\overset{\phi}{\rightrightarrows}} \mathrm{Gal}(L/K)$$

and both send every uniformizer of K_v^* to Frob_v. Then $\phi = \phi'$.

Lemma 6.1. Let $S \subseteq V_K$ be a finite set of places. Let $\mathbb{I}_K^S := \{x = (x_v) \in \mathbb{I}_K \mid x_v = 1 \text{ for all } v \in S\}$. Then the image of $\mathbb{I}_K^S$ in C_K is dense.

Proof. For any $x = (x_v) \in \mathbb{I}_K$ and any open neighborhood U of x, we want to show that

$(\mathbb{I}_K^S \cdot K^*) \cap U \neq \emptyset$. We may assume the neighborhood U is of the form

$$U = \prod_{v \in T} U_v \times \prod_{v \notin T} \mathcal{O}_{K_v}^*$$

for some finite set T containing S, where each U_v is an open neighborhood of x_v. By the Weak Approximation Theorem, there exists $y \in K^*$ such that $y \in U_v$ for all $v \in T$.

Now, let's choose an idele $z = (z_v)$ such that:

- $z_v = 1$ for all $v \in S$.
- $yz_v \in \mathcal{O}_{K_v}^*$ for all $v \notin S$.

By construction, $z \in \mathbb{I}_K^S$ and $yz \in U$, which means $yz \in (\mathbb{I}_K^S \cdot K^*) \cap U \neq \emptyset$. □

Proof of Proposition. It suffices to show these two composite maps coincide on the dense subset $\mathbb{I}_K^S$ of C_K by **Lemma 6.1**.

For all $x \in \mathbb{I}_K^S$, we want to show $\phi(x) = \phi'(x)$. Choose a finite set of places $T \subseteq V_K$, such that $S \subseteq T$ and:

1. $x_v \in \mathcal{O}_{K_v}^*$ for all $v \notin T$.
2. $\prod_{v \in T}\{1\} \times \prod_{v \notin T} \mathcal{O}_{K_v}^* \subseteq \operatorname{Ker}\phi \cap \operatorname{Ker}\phi'$ (This is in fact open).

(Remark: $\operatorname{Ker}\phi$ and $\operatorname{Ker}\phi'$ are open because $\mathrm{Gal}(L/K)$ is equipped with discrete topology and the continuousness of ϕ and ϕ'.)

Let $i_v : K_v^* \to \mathbb{I}_K$ be the canonical inclusion.

$$\begin{aligned}\phi(x) &= \prod_{v \in T} \phi(i_v(x_v)) \\ &= \prod_{v \in T \setminus S} \phi(i_v(x_v)) = \prod_{v \in T \setminus S} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)} \\ &= \prod_{v \in V_K \setminus S} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)} = \phi'(x). \qquad \square\end{aligned}$$

□

6.1 Functoriality of global Artin map

Theorem 6.1 (**Norm functoriality**)**.** Let L/K be a finite abelian extension. The following diagram is commutative:

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_L} & \mathrm{Gal}(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ C_K & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

where $\mathrm{Gal}(L^{ab}/L) \to \mathrm{Gal}(K^{ab}/K)$ is induced as shown below:

$$\begin{array}{ccc} \mathrm{Gal}(\bar{K}/L) & \hookrightarrow & \mathrm{Gal}(\bar{K}/K) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L^{ab}/L) & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \end{array}$$

Remark: For a topological group G, its abelianization is defined as

$$G^{ab,t} := G/\overline{[G,G]}$$

where $\overline{[G,G]}$ is the closure of the derived subgroup of G. This is the maximal quotient abelian topological group of G.

Proof. It suffices to show the functoriality on the finite level. Suppose K'/K is a finite abelian extension. Then $K'L/L$ is also a finite abelian extension. Write $L' := K'L$. It suffices to show the following diagram commutes:

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_{L'/L}} & \mathrm{Gal}(L'/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \theta} \\ C_K & \xrightarrow{\psi_{K'/K}} & \mathrm{Gal}(K'/K) \end{array}$$

By **Lemma 6.1**, it suffices to show there exists a finite set $\widetilde{T} \subseteq V_K$ such that the following diagram is commutative for all places $w \in V_L \setminus \widetilde{T}$.

$$\begin{array}{ccccccc} L_w^* & \hookrightarrow & \mathbb{I}_L^{\widetilde{T}} & \longrightarrow & C_L & \xrightarrow{\psi_{L'/L}} & \mathrm{Gal}(L'/L) \\ & & & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \theta} \\ & & & & C_K & \xrightarrow{\psi_{K'/K}} & \mathrm{Gal}(K'/K) \end{array}$$

We have proved in an exercise: There is a local diagram :

$$\begin{array}{ccc} L_w^* & \xrightarrow{i_w} & C_L \\ {\scriptstyle N_{w/v}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K_v^* & \xrightarrow{i_v} & C_K \end{array}$$

Here we chose a finite set of places $T \subseteq V_K$ such that T contains all places $v \in V_K$ that ramify in K', and all archimedean places $V_{K,\infty}$. Let $\widetilde{T} = \mathrm{pr}_L^{-1}(T)$, where $\mathrm{pr}_L : V_L \to V_K$ is the map restricting places from L to K. Here $w \in V_L \setminus \widetilde{T}$ and $v = \mathrm{pr}_L(w) \in V_K \setminus T$.

Let $\pi_w \in L_w^*$ be a uniformizer. The local Artin map sends $\pi_w \mapsto \mathrm{Frob}_w$. Similarly, $\pi_v \mapsto \mathrm{Frob}_v$. The norm of the uniformizer is given by

$$N_{L_w/K_v}(\pi_w) = \mathrm{unit} \cdot \pi_v^{f(w|v)}. \quad \text{Note: } [L_w : K_v] = e(w|v)f(w|v).$$

Applying the local Artin map ψ_v to the norm gives:

$$\begin{aligned} \psi_v(N_{L_w/K_v}(\pi_w)) &= \psi_v(\mathrm{unit} \cdot \pi_v^{f(w|v)}) \\ &= \psi_v(\pi_v)^{f(w|v)} = \mathrm{Frob}_v^{f(w|v)}. \end{aligned}$$

So it remains to show that $\theta(\mathrm{Frob}_w) = \mathrm{Frob}_v^{f(w|v)}$.

We know that $\mathrm{Frob}_w(x) \equiv x^{q_1} \pmod{\mathfrak{P}_w}$ where $q_1 = |k_w|$, the size of the residue field of L_w. And $\mathrm{Frob}_v(x) \equiv x^{q_2} \pmod{\mathfrak{p}_v}$ where $q_2 = |k_v|$. The inertia degree is defined by the relation between the residue field sizes: $q_1 = q_2^{f(w|v)}$. For any $x \in K$:

$$\begin{aligned} \theta(\mathrm{Frob}_w)(x) &\equiv \mathrm{Frob}_w(x) \equiv x^{q_1} \equiv x^{q_2^{f(w|v)}} \pmod{\mathfrak{p}_v} \\ &\equiv \mathrm{Frob}_v^{f(w|v)}(x) \pmod{\mathfrak{p}_v}. \end{aligned}$$

So we have $\theta(\mathrm{Frob}_w) = \mathrm{Frob}_v^{f(w|v)}$.

(Note: We need to choose unramified places to define Frobenius elements!) □

Theorem 6.2. The following diagram, relating the Artin maps for fields L and K where L/K is a finite extension, is commutative:

$$\begin{array}{ccc} C_K & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{ab}/K) \\ {\scriptstyle\eta}\big\uparrow & & \big\downarrow{\scriptstyle\mathrm{Ver}} \\ C_L & \xrightarrow{\psi_L} & \mathrm{Gal}(L^{ab}/L) \end{array}$$

Remark: Here the map $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L^{ab}/L)$ is induced by the transfer map (Verlagerung) which will be definied later:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \xrightarrow{\mathrm{Ver}} & \mathrm{Gal}(\overline{K}/L) \\ \big\downarrow{\scriptstyle\mathrm{Res}} & & \big\downarrow{\scriptstyle\mathrm{Res}} \\ \mathrm{Gal}(K^{ab}/K) & \xrightarrow{\mathrm{Ver}} & \mathrm{Gal}(L^{ab}/L) \end{array}$$

Definition 6.1 (**Transfer Map**)**.** Let G be a group and $H < G$ be a subgroup of finite index. We define the transfer map (Verlagerung), which is a group homomorphism $\mathrm{Ver} : G^{ab} \to H^{ab}$.

- **Abstract way:** via group homology theory. The transfer map is the restriction map on the first homology groups:

$$\begin{array}{ccc} H_1(G;\mathbb{Z}) & \longrightarrow & H_1(H;\mathbb{Z}) \\ \cong & & \cong \\ G^{ab} & & H^{ab} \end{array}$$

- **Explicit way:** It suffices to define a group homomorphism $G \to H^{ab}$. Let $[G : H] = n$. Write a right coset decomposition $G = \coprod_{i=1}^{n} Ha_i$. For any $g \in G$, there exists a unique permutation $\sigma_g \in S_n$ such that $Ha_i g = Ha_{\sigma_g(i)}$ for all $i \in \{1, \ldots, n\}$. Write $a_i g = h_{i,g} a_{\sigma_g(i)}$ with $h_{i,g} \in H$. Define $\mathrm{Ver}(g) := \prod_{i=1}^{n} h_{i,g} \pmod{H^{der}}$.

Claim: $\mathrm{Ver} : G \to H^{ab}$ is a group homomorphism.

proof of claim. For any $g_1, g_2 \in G$:

$$\begin{aligned} a_i(g_1 g_2) &= (a_i g_1) g_2 \\ &= (h_{i,g_1} a_{\sigma_{g_1}(i)}) g_2 \\ &= h_{i,g_1} (a_{\sigma_{g_1}(i)} g_2) \\ &= h_{i,g_1} h_{\sigma_{g_1}(i),g_2} a_{\sigma_{g_2}(\sigma_{g_1}(i))} \end{aligned}$$

So $h_{i,g_1g_2} = h_{i,g_1} h_{\sigma_{g_1}(i),g_2}$. Then

$$\begin{aligned}
\mathrm{Ver}(g_1g_2) &= \prod_{i=1}^{n} h_{i,g_1g_2} \pmod{H^{der}} \\
&= \prod_{i=1}^{n} h_{i,g_1} h_{\sigma_{g_1}(i),g_2} \pmod{H^{der}} \\
&\equiv \left(\prod_{i=1}^{n} h_{i,g_1}\right)\left(\prod_{i=1}^{n} h_{\sigma_{g_1}(i),g_2}\right) \pmod{H^{der}} \\
&\equiv \left(\prod_{i=1}^{n} h_{i,g_1}\right)\left(\prod_{j=1}^{n} h_{j,g_2}\right) \pmod{H^{der}} \quad (\text{since } \sigma_{g_1} \text{ is a permutation}) \\
&= \mathrm{Ver}(g_1)\cdot \mathrm{Ver}(g_2).
\end{aligned}$$

□

Exercise 6.1. 1. Check that the definition of the transfer map doesn't depend on the choice of representatives of $H \setminus G$.

2. Let G be a topological group, H an open subgroup of finite index. Show that $\mathrm{Ver} : G^{ab} \to H^{ab}$ induces a continuous homomorphism $\mathrm{Ver} : G^{ab,t} \to H^{ab,t}$.($G^{ab,t}$ is definied in the **Remark** after Theorem 6.2)

6.2 Local Class Field Theory

Theorem 6.3 (**Local Reciprocity**)**.** Let K be a p-adic field. There is a continuous homomorphism $\psi_K : K^* \to \mathrm{Gal}(K^{ab}/K)$ with dense image, which is called the local Artin map, satisfying: For each finite abelian extension L/K, consider the composite map

$$\psi_{L/K} : K^* \xrightarrow{\psi_K} \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

(1) $\psi_{L/K}$ is surjective with $\ker(\psi_{L/K}) = N_{L/K}(L^*)$.

(2) If L/K is unramified, then $\psi_{L/K}$ sends every uniformizer of K to Frob elements.

Remark: The reciprocity law is trivial for $K = \mathbb{R}$ or $\mathbb{C}$.

- For $K = \mathbb{R}$, the only non-trivial extension is $\mathbb{C}/\mathbb{R}$. We have the isomorphism:

$$\mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) \cong \mathbb{R}^*/\mathbb{R}_{>0} \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

- For $K = \mathbb{C}$, there are no non-trivial finite abelian extensions, so $\mathrm{Gal}(\mathbb{C}^{ab}/\mathbb{C}) = \{1\}$.

Remark: For a finite abelian extension L/K, the local reciprocity law gives a fundamental isomorphism:

$$K^*/N_{L/K}(L^*) \cong \mathrm{Gal}(L/K)$$

This implies that the index of the norm subgroup equals the degree of the extension:

$$[K^* : N_{L/K}(L^*)] = [L : K]$$

Theorem 6.4 (**Local Existence Theorem**)**.** A subgroup of K^* is open of finite index if and only if it is of the form $N_{L/K}(L^*)$ for some finite abelian extension L/K.

Corollary 6.2 (**Classification of abelian extensions**)**.** There is an inclusion-reversing bijection:

$$\{\text{finite abelian extensions of } K\} \longleftrightarrow \{\text{open finite index subgroups of } K^*\}$$
$$L \longmapsto N_{L/K}(L^*)$$

Proof. Same argument as the global case. □

Remark: From the following exercise, we know that: For all integers $n \geq 1$, there exists a unique unramified extension K_n/K of degree n.

Exercise 6.2. Show that for the unramified extension K_n/K:

1. $N_{K_n/K}(\mathcal{O}_{K_n}^*) = \mathcal{O}_K^*$.
2. This implies $N_{K_n/K}(K_n^*) = \pi^{n\mathbb{Z}} \times \mathcal{O}_K^*$, where π is a uniformizer of K.

By the above exercise, in the correspondence in **Corollary 6.2**, we have:

$$K_n \longleftrightarrow \pi^{n\mathbb{Z}} \times \mathcal{O}_K^*$$

Proposition 6.2. The local Artin map is unique.

Proof. Let ψ_K, ψ'_K be two such maps. We want to show $\psi_{L/K} = \psi'_{L/K}$ for every finite abelian extension L/K.

It suffices to show $\psi_K(\pi) = \psi'_K(\pi)$ for a uniformizer π of K.

Step 1. It suffices to deal with finite abelian extensions L/K such that $N_{L/K}(L^*) = \pi^{n\mathbb{Z}} \times U_K^m$ for some $n \geq 1, m \geq 0$. Here, $U_K^0 = \mathcal{O}_K^*$ and $U_K^i = 1 + \mathfrak{m}_K^i$ for all $i \geq 1$.

This is because: For any finite abelian extension L/K, $N_{L/K}(L^*)$ is an open subgroup of K^* of finite index. Therefore, it must contain a subgroup of the form $\pi^{n\mathbb{Z}} \times U_K^m$. By the classification of finite extensions, this implies L is a subfield of the extension L' corresponding to this subgroup, where $L' = L_{n,m}$ for $n, m \geq 1$.

The argument then proceeds by relating the maps for L to the maps for L' via the natural projection $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$.

Step 2. The norm group for the extension $L_{n,m}/K$ is

$$\begin{aligned} N_{L_{n,m}/K}(L_{n,m}^*) &= \pi^{n\mathbb{Z}} \times U_K^m \\ &= (\pi^{n\mathbb{Z}} \times \mathcal{O}_K^*) \cap (\pi^{\mathbb{Z}} \times U_K^m) \\ &= N_{K_n/K}(K_n^*) \cap N_{E_m/K}(E_m^*) \end{aligned}$$

where K_n is the unramified extension of degree n and E_m is the class field for the open subgroup $\pi^{\mathbb{Z}} \times U_K^m$ of finite index, which exists by the Existence Theorem.

This implies that the class field $L_{n,m}$ is the composite field $E_m \cdot K_n$. We have an injective homomorphism from the Galois group of the composite field:

$$\psi_{L_{n,m}/K} : K^* \to \mathrm{Gal}(L_{n,m}/K) \hookrightarrow \mathrm{Gal}(E_m/K) \times \mathrm{Gal}(K_n/K)$$

This map is given by $a \mapsto (\psi_{E_m/K}(a), \psi_{K_n/K}(a))$. The kernel of this map is $\ker(\psi_{E_m/K}) \cap \ker(\psi_{K_n/K})$.

It remains to show $\psi_{E_m/K}(\pi) = \psi'_{E_m/K}(\pi)$. The equality $\psi_{K_n/K}(\pi) = \psi'_{K_n/K}(\pi)$ is a FACT from the properties of the Artin map for unramified extensions (Artin reciprocity). For a uniformizer π, we have $\psi_{E_m/K}(\pi) = 1$ because $\pi \in N_{E_m/K}(E_m^*) = \ker \psi_{E_m/K}$, and similarly for ψ'. □

Remark: The extension E_m/K is totally ramified. Indeed, if not, then there is an intermediate field $K \subseteq K_d \subseteq E_m$ where K_d/K is an unramified extension of degree $d \geq 2$.

By the functoriality of the norm map, we would have

$$N_{E_m/K}(E_m^*) \subseteq N_{K_d/K}(K_d^*)$$

which implies

$$\pi^{\mathbb{Z}} \times U_K^m \subseteq \pi^{d\mathbb{Z}} \times \mathcal{O}_K^*$$

This is impossible! □

Corollary 6.3. The following diagram is commutative:

$$\begin{array}{ccc} K^* & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow{\scriptstyle \mathrm{ord}} & & \downarrow{\scriptstyle \mathrm{pr}} \\ \mathbb{Z} & \hookrightarrow & \hat{\mathbb{Z}} \simeq \mathrm{Gal}(K^{ur}/K) \end{array}$$

Here we have an isomorphism

$$\hat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(K^{ur}/K)$$

where K^{ur}/K is the maximal unramified extension of K. The map sends $1 \mapsto \mathrm{Frob}$.

Proof. Consider any uniformizer π of K. From the Local Reciprocity Theorem, the commutativity follows from the fact that under the two compositions, π is simultaneously sent to the Frobenius element.

$$\begin{array}{ccc} \pi & \longmapsto & * \\ \downarrow & & \downarrow \\ 1 & \longmapsto & \mathrm{Frob} \end{array}$$

□

Definition 6.2. Let $\mathrm{pr} : \mathrm{Gal}(K^{ab}/K) \to \hat{\mathbb{Z}}$ be the projection.

- The **Weil group** of K is defined as $W_K^{ab} := \mathrm{pr}^{-1}(\mathbb{Z})$.
- The **inertia subgroup** of K is defined as $I_K := \ker(\mathrm{pr}) \trianglelefteq \mathrm{Gal}(K^{ab}/K)$.

Corollary 6.4. We have the following commutative diagram with exact rows, and the vertical maps are isomorphisms of topological groups.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & K^* & \xrightarrow{\text{ord}} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow\cong & & \psi_K\downarrow\cong & & \| & & \\ 0 & \longrightarrow & I_K & \longrightarrow & W_K^{ab} & \xrightarrow{\text{pr}} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

Proof. To show $\psi_K : K^* \to W_K^{ab}$ is an isomorphism, it suffices to show that the restriction $\psi_K|_{\mathcal{O}_K^*}$ is an isomorphism onto I_K.

- $\psi|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to I_K$ is injective.

  We have

$$\begin{aligned} \ker(\psi_K) &= \bigcap_{L/K \text{ finite abelian extension}} \ker(\psi_{L/K}) \\ &= \bigcap_{H \le K^* \text{ open subgroup of finite index}} H \end{aligned}$$

Any open subgroup H must contain a subgroup of the form $U_K^m \times \pi^{n\mathbb{Z}}$ for some m, n. The intersection of all such subgroups is $\{1\}$. This implies $\ker(\psi_K) \cap \mathcal{O}_K^* = \{1\}$.

- $\psi|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to I_K$ is surjective.

- **Claim:** The image $\psi_K(\mathcal{O}_K^*)$ is dense in I_K.

proof of claim. We will prove it in the sight of convergence. The sight is reasonable because all those groups are Hausdorff topological groups.

Let $g \in I_K$. We want to show there exists a sequence $\{x_n\} \subseteq \mathcal{O}_K^*$ such that $\psi_K(x_n) \to g$ as $n \to \infty$. Because the Local Reciprocity Theorem, there exists a sequence $\{y_n\} \subseteq K^*$ such that $\psi_K(y_n) \to g$ as $n \to \infty$. So the sequence $\{\iota \circ \text{ord}(y_n)\}$ in $\hat{\mathbb{Z}} \simeq \text{Gal}(K^{ur}/K)$ converges to $\text{pr}(g) = 0$.

Note that $\text{ord}(y_n) \in \mathbb{Z} \subseteq \hat{\mathbb{Z}}$. By analyzing the topology of $\hat{\mathbb{Z}}$, the convergence is equivalent to:

$$\text{For all } m \ge 1, \text{exists } N \text{ such that } n \ge N \text{ implies } \text{ord}(y_n) \equiv 0 \pmod{m}.$$

π is a uniformizer of K. We **claim**: In $\text{Gal}(K^{ab}/K)$, the sequence $\{\psi_K(\pi^{-\text{ord}(y_n)})\}$ converges to 1 as $n \to \infty$. It is equivalent to show that for all open subgroups $U \subseteq \text{Gal}(K^{ab}/K)$, the sequence $\{\overline{\psi_K(\pi^{-\text{ord}(y_n)})}\}$ converges to $\overline{1}$ in $\text{Gal}(K^{ab}/K)/U$.

For any open subgroup $U \subseteq \mathrm{Gal}(K^{ab}/K)$, we know that $[\mathrm{Gal}(K^{ab}/K) : U] < \infty$. Let $m = [\mathrm{Gal}(K^{ab}/K) : U]$. By the above convergence condition on $\mathrm{ord}(y_n)$, there exists N such that for all $n \geq N$, $\mathrm{ord}(y_n) \equiv 0 \pmod{m}$. Therefore, for all $n \geq N$,

$$\overline{\psi_K(\pi^{-\mathrm{ord}(y_n)})} = \overline{1} \in \mathrm{Gal}(K^{ab}/K)/U.$$

This proves the claim.

Now define $x_n := y_n \cdot \pi^{-\mathrm{ord}(y_n)} \in \mathcal{O}_K^*$. We have

$$\psi_K(x_n) = \psi_K(y_n) \cdot \psi_K(\pi^{-\mathrm{ord}(y_n)}).$$

converges to $g \cdot 1 = g$ as $n \to \infty$. So the image $\psi_K(\mathcal{O}_K^*)$ is dense in I_K. □

Since $\mathcal{O}_K^*$ is compact and ψ_K is continuous, the image $\psi_K(\mathcal{O}_K^*)$ is compact. The inertia group I_K is a profinite group, hence compact and Hausdorff. In a Hausdorff space, a compact (and therefore closed) dense subset of a topological space is the space itself. Thus, $\psi_K(\mathcal{O}_K^*) = I_K$.

- $\psi_K : K^* \to W_K^{ab}$ is a homeomorphism.

We have the following isomorphisms of topological groups:

$$\begin{array}{ccc} K^* & \xrightarrow{\cong} & \mathcal{O}_K^* \times \mathbb{Z} \\ \downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \cong} \\ W_K^{ab} & \xrightarrow{\cong} & I_K \times \mathbb{Z} \end{array}$$

The map $\psi_K|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to I_K$ is a continuous bijection from a compact space to a Hausdorff space, and therefore is a homeomorphism. Thus, the map ψ_K is a homeomorphism. □

6.3 Homework

Homework 6.1.

1. Show that the definition of the transfer map $\mathrm{Ver} : G^{ab} \to H^{ab}$ doesn't depend on the choice of representatives for the cosets $H \setminus G$.

2. When G is abelian, show that $\mathrm{Ver}(g) = g^{[G:H]}$ for any $g \in G$.

3. Let G be a topological group and H be an open subgroup of G of finite index. Show that $\mathrm{Ver} : G^{ab} \to H^{ab}$ induces a continuous homomorphism $\mathrm{Ver} : G^{ab,t} \to H^{ab,t}$, where $(G)^{ab,t}$ denotes the abelianization as a topological group (i.e. G modulo the closure of the derived subgroup).

4. Let $\tilde{G}$ be a quotient group of G and let $\tilde{H}$ be the image of H in $\tilde{G}$. Assume that the natural map $G/H \to \tilde{G}/\tilde{H}$ is a bijection. Show that we have a commutative diagram

$$\begin{array}{ccc} G^{ab} & \xrightarrow{\mathrm{Ver}} & H^{ab} \\ \downarrow & & \downarrow \\ \tilde{G}^{ab} & \xrightarrow{\mathrm{Ver}} & \tilde{H}^{ab}. \end{array}$$

   Do we still have this commutative diagram without the coset bijective assumption?

proof of 1. Let G be a group and H a subgroup of finite index $n = [G : H]$. The transfer map $\mathrm{Ver} : G \to H^{ab} = H/[H, H]$ is defined as follows. Let $\{t_1, \ldots, t_n\}$ be a set of right coset representatives of H in G. For any $g \in G$, right multiplication by g permutes the cosets. This action defines a permutation $\sigma \in S_n$ such that $Ht_ig = Ht_{\sigma(i)}$. This implies that for each i, there is a unique $h_i \in H$ such that $t_ig = h_it_{\sigma(i)}$. The transfer is then defined as $\mathrm{Ver}(g) = \prod_{i=1}^n h_i \pmod{[H, H]}$.

Now, let $\{s_1, \ldots, s_n\}$ be another set of right coset representatives. Since they represent the same cosets, for each i there exists $k_i \in H$ such that $s_i = k_it_i$. Let's define the transfer using this new set of representatives. For $g \in G$, there is a permutation $\pi \in S_n$ and elements $h'_i \in H$ such that $s_ig = h'_is_{\pi(i)}$.

We want to show that $\prod_{i=1}^n h_i \equiv \prod_{i=1}^n h'_i \pmod{[H, H]}$. Substitute $s_i = k_it_i$ into the second definition:

$$(k_it_i)g = h'_i(k_{\pi(i)}t_{\pi(i)})$$

Now substitute $t_i g = h_i t_{\sigma(i)}$:

$$k_i(h_i t_{\sigma(i)}) = h'_i k_{\pi(i)} t_{\pi(i)}$$

Since $\{t_j\}$ is a set of representatives for disjoint cosets, we must have $\sigma(i) = \pi(i)$ for all i, which implies the permutations are the same, $\sigma = \pi$. The relation between the elements of H is then:

$$k_i h_i = h'_i k_{\sigma(i)} \implies h'_i = k_i h_i k_{\sigma(i)}^{-1}$$

Now we compute the product of the h'_i in the abelian group H^{ab}:

$$\prod_{i=1}^{n} [h'_i] = \prod_{i=1}^{n} [k_i h_i k_{\sigma(i)}^{-1}] = \left(\prod_{i=1}^{n} [k_i]\right)\left(\prod_{i=1}^{n} [h_i]\right)\left(\prod_{i=1}^{n} [k_{\sigma(i)}^{-1}]\right)$$

Since σ is a permutation of $\{1, \ldots, n\}$, the set $\{k_{\sigma(1)}, \ldots, k_{\sigma(n)}\}$ is a reordering of $\{k_1, \ldots, k_n\}$. As we are in an abelian group, the product is unaffected by the order:

$$\prod_{i=1}^{n} [k_{\sigma(i)}] = \prod_{i=1}^{n} [k_i] \implies \prod_{i=1}^{n} [k_{\sigma(i)}^{-1}] = \left(\prod_{i=1}^{n} [k_{\sigma(i)}]\right)^{-1} = \left(\prod_{i=1}^{n} [k_i]\right)^{-1}$$

Substituting this back, we get:

$$\prod_{i=1}^{n} [h'_i] = \left(\prod_{i=1}^{n} [k_i]\right)\left(\prod_{i=1}^{n} [h_i]\right)\left(\prod_{i=1}^{n} [k_i]\right)^{-1} = \prod_{i=1}^{n} [h_i]$$

Thus, the definition of the transfer map is independent of the choice of coset representatives. □

proof of 2. If G is abelian, then H is also abelian, so $H^{ab} = H$. The defining relation is $t_i g = h_i t_{\sigma(i)}$. Since G is abelian, $t_i g = g t_i$. So, $g t_i = h_i t_{\sigma(i)}$. This implies that $t_{\sigma(i)}$ and $g t_i$ are in the same coset of H.

$$H t_{\sigma(i)} = H g t_i = g H t_i$$

The permutation σ corresponds to the multiplication by g in the quotient group G/H. The element h_i is given by $h_i = g t_i t_{\sigma(i)}^{-1}$. The transfer is the product of these h_i:

$$\mathrm{Ver}(g) = \prod_{i=1}^{n} h_i = \prod_{i=1}^{n} (g t_i t_{\sigma(i)}^{-1})$$

Since G is abelian, we can rearrange the terms in the product:

$$\mathrm{Ver}(g) = \left(\prod_{i=1}^{n} g\right)\left(\prod_{i=1}^{n} t_i\right)\left(\prod_{i=1}^{n} t_{\sigma(i)}^{-1}\right) = g^n \left(\prod_{i=1}^{n} t_i\right)\left(\prod_{i=1}^{n} t_{\sigma(i)}\right)^{-1}$$

Since σ is a permutation, the set $\{t_{\sigma(1)}, \ldots, t_{\sigma(n)}\}$ is the same as $\{t_1, \ldots, t_n\}$. Because G is abelian, the product of the elements is the same regardless of order.

$$\prod_{i=1}^{n} t_{\sigma(i)} = \prod_{i=1}^{n} t_i$$

Therefore, the expression simplifies to:

$$\mathrm{Ver}(g) = g^n \left(\prod_{i=1}^{n} t_i\right)\left(\prod_{i=1}^{n} t_i\right)^{-1} = g^n \cdot e = g^n$$

□

proof of 3. Let G be a topological group and H be an open subgroup of finite index n.

- **Continuity of** $\mathrm{Ver}_0 : G \to H^{ab}$

$\pi : H \to H^{ab,t}$ is the quotient map, which is continuous. For any $\widetilde{U} \subseteq H^{ab,t}$ open subset and given a $g \in G$ such that $\mathrm{Ver}_0(g) \in \widetilde{U}$, $a_1, \ldots, a_n$ are representatives of the right cosets of H in G. Then there exists $h_i \in H$ and $\sigma \in S_n$ such that $a_i g = h_i a_{\sigma(i)}$.

We have:

$$\begin{aligned} h_1 h_2 \ldots h_n &\in \pi^{-1}(\widetilde{U}) \\ e \in U_0 &:= h_n^{-1} h_{n-1}^{-1} \ldots h_1^{-1} \pi^{-1}(\widetilde{U}) \subseteq H \end{aligned}$$

U_0 is an open subset of H containing e. Consider:

$$U_1 := U_0 \cap U_0 \underbrace{U_0^{-1} \ldots U_0^{-1}}_{(n-1) \text{ times}}$$

It is also an open subset of H containing e. Then:

$$\begin{aligned} \pi((h_1 U_1)(h_2 U_1) \ldots (h_n U_1)) &= \pi(h_1 h_2 \ldots h_n)\pi(U_1^n) \\ &\subseteq \pi(h_1 h_2 \ldots h_n)\pi(U_1 U_0 \ldots U_0) \\ &\subseteq \pi(h_1 h_2 \ldots h_n)\pi(U_0) \\ &\subseteq \widetilde{U} \end{aligned}$$

Consider the open subset of G:

$$\bigcap_{i=1}^{n} a_i^{-1}(h_i U_1) a_{\sigma(i)}$$

For any $g' \in \bigcap_{i=1}^{n} a_i^{-1}(h_i U_1) a_{\sigma(i)}$:

$$\begin{aligned} \mathrm{Ver}_0(g') &\in \pi((h_1U_1)(h_2U_1)\dots(h_nU_1)) \\ &\subseteq \widetilde{U} \end{aligned}$$

And for any $i \in [1, n]$, obviously $g \in a_i^{-1}(h_i U_1) a_{\sigma(i)}$. So:

$$g \in \bigcap_{i=1}^{n} a_i^{-1}(h_i U_1) a_{\sigma(i)} \subseteq \mathrm{Ver}_0^{-1}(\widetilde{U})$$

This shows that Ver_0 is continuous.

- **Induced map on topological abelianizations**:

We want to show that Ver_0 induces a continuous homomorphism $\mathrm{Ver} : G^{ab,t} \to H^{ab,t}$, where $G^{ab,t} = G/\overline{[G,G]}$ and $H^{ab,t} = H/\overline{[H,H]}$.

First we prove $\overline{[G,G]} \subseteq \ker \mathrm{Ver}_0$. We have proved in class that $[G,G] \subseteq \ker(\mathrm{Ver}_0)$. $H \setminus \overline{[H,H]}$ is open in H, so $\pi(H \setminus \overline{[H,H]}) = H^{ab,t} \setminus \{\bar{e}\}$ is open in $H^{ab,t}$, i.e. $\{\bar{e}\}$ is closed in $H^{ab,t}$. Therefore $\ker(\mathrm{Ver}_0) = \mathrm{Ver}_0^{-1}(\{\bar{e}\})$ is closed in G. This implies $\overline{[G,G]} \subseteq \ker(\mathrm{Ver}_0)$.

Thus, for $\mathrm{Ver} : G^{ab,t} \to H^{ab,t}$ and open subset $\widetilde{U} \subseteq H^{ab,t}$, denote quotient map $p : G \to G^{ab,t}$, then:

$$\mathrm{Ver}^{-1}(\widetilde{U}) = p(\mathrm{Ver}_0^{-1}(\widetilde{U}))$$

where $\mathrm{Ver}_0^{-1}(\widetilde{U})$ is open in G and p is an open map, so Ver is continuous. □

proof of 4. Let $\phi : G \to \tilde{G}$ be the quotient map. Let $\psi : H \to \tilde{H}$ be the restriction of ϕ to H. These induce homomorphisms on the abelianizations, $\phi_* : G^{ab} \to \tilde{G}^{ab}$ and $\psi_* : H^{ab} \to \tilde{H}^{ab}$. We need to show that $\psi_* \circ \mathrm{Ver}_G = \mathrm{Ver}_{\tilde{G}} \circ \phi_*$.

$$\begin{array}{ccc} G^{ab} & \xrightarrow{\mathrm{Ver}_G} & H^{ab} \\ \downarrow{\scriptstyle \phi_*} & & \downarrow{\scriptstyle \psi_*} \\ \tilde{G}^{ab} & \xrightarrow{\mathrm{Ver}_{\tilde{G}}} & \tilde{H}^{ab} \end{array}$$

Let $g \in G$. Let $\{t_1, \dots, t_n\}$ be a set of right coset representatives for H in G. The assumption

that the map $G/H \to \tilde{G}/\tilde{H}$ is a bijection means that $[\tilde{G} : \tilde{H}] = [G : H] = n$ and that $\{\tilde{t}_1, \ldots, \tilde{t}_n\}$, where $\tilde{t}_i = \phi(t_i)$, is a valid set of right coset representatives for $\tilde{H}$ in $\tilde{G}$.

Let's compute the path starting from the top left:

1. $\mathrm{Ver}_G(g)$: We have $t_i g = h_i t_{\sigma(i)}$ for $h_i \in H$. So $\mathrm{Ver}_G(g) = [\prod h_i] \in H^{ab}$.
2. $\psi_*(\mathrm{Ver}_G(g))$: We apply ψ_*, which is induced by ϕ. This gives $[\phi(\prod h_i)] = [\prod \phi(h_i)] = [\prod \tilde{h}_i] \in \tilde{H}^{ab}$, where $\tilde{h}_i = \phi(h_i) \in \tilde{H}$.

Now let's compute the other path, starting from the bottom left:

1. $\phi_*(g)$: This gives the element $\tilde{g} = \phi(g) \in \tilde{G}$.
2. $\mathrm{Ver}_{\tilde{G}}(\phi(g))$: We use the representatives $\{\tilde{t}_1, \ldots, \tilde{t}_n\}$. We need to find $\tilde{h}'_i \in \tilde{H}$ and a permutation π such that $\tilde{t}_i \tilde{g} = \tilde{h}'_i \tilde{t}_{\pi(i)}$. Let's apply the homomorphism ϕ to the relation from the first calculation:

$$\begin{aligned} \phi(t_i g) &= \phi(h_i t_{\sigma(i)}) \\ \phi(t_i)\phi(g) &= \phi(h_i)\phi(t_{\sigma(i)}) \\ \tilde{t}_i \tilde{g} &= \tilde{h}_i \tilde{t}_{\sigma(i)} \end{aligned}$$

   This is exactly the defining relation for the transfer map in $\tilde{G}$. By uniqueness, the permutation must be $\pi = \sigma$ and the elements from $\tilde{H}$ must be $\tilde{h}'_i = \tilde{h}_i$. Therefore, $\mathrm{Ver}_{\tilde{G}}(\tilde{g}) = [\prod \tilde{h}'_i] = [\prod \tilde{h}_i] \in \tilde{H}^{ab}$.

Since both paths yield the same result, the diagram commutes.

- **Do we still have this commutative diagram without the coset bijective assumption?**

No, the diagram does not commute in general if the map $G/H \to \tilde{G}/\tilde{H}$ is not a bijection.

Consider the following counterexample where G is abelian. In this case, $\mathrm{Ver}_G(g) = g^{[G:H]}$ and $\mathrm{Ver}_{\tilde{G}}(\tilde{g}) = \tilde{g}^{[\tilde{G}:\tilde{H}]}$. Let $n = [G : H]$ and $m = [\tilde{G} : \tilde{H}]$. The commutativity of the diagram for an element $g \in G$ is equivalent to the condition $\psi_*(\mathrm{Ver}_G(g)) = \mathrm{Ver}_{\tilde{G}}(\phi_*(g))$. Let's evaluate both sides:

- LHS: $\psi_*(\mathrm{Ver}_G(g)) = \psi_*(g^n) = \phi(g^n) = \phi(g)^n = \tilde{g}^n$.
- RHS: $\mathrm{Ver}_{\tilde{G}}(\phi_*(g)) = \mathrm{Ver}_{\tilde{G}}(\tilde{g}) = \tilde{g}^m$.

So, for the diagram to commute for all g, we need $\tilde{g}^n = \tilde{g}^m$ for all $\tilde{g} \in \tilde{G}$. This is not always true if $n \neq m$.

Let $G = \mathbb{Z}$, $K = 6\mathbb{Z}$, and $H = 4\mathbb{Z}$.

- $n = [G : H] = [\mathbb{Z} : 4\mathbb{Z}] = 4$.
- $\tilde{G} = G/K = \mathbb{Z}/6\mathbb{Z}$.
- $\tilde{H} = (H + K)/K = (4\mathbb{Z} + 6\mathbb{Z})/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z}$, which is the subgroup $\langle 2 \rangle = \{0, 2, 4\}$ in $\mathbb{Z}_6$.
- $m = [\tilde{G} : \tilde{H}] = [(\mathbb{Z}/6\mathbb{Z}) : (2\mathbb{Z}/6\mathbb{Z})] = 2$.

Here $n = 4$ and $m = 2$, so the map on cosets is not a bijection. Let's check the commutativity condition for $g = 1 \in \mathbb{Z}$. The image of g in $\tilde{G}$ is $\tilde{g} = 1 \pmod 6$.

- LHS: $\tilde{g}^n = 1^4 = 4 \cdot 1 = 4 \pmod 6$.
- RHS: $\tilde{g}^m = 1^2 = 2 \cdot 1 = 2 \pmod 6$.

Since $4 \not\equiv 2 \pmod 6$, the diagram does not commute for $g = 1$. □

Homework 6.2. Let L/K be a finite unramified extension of p-adic fields. Let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$ and let k_K be the residue field of K. Let $U_K^0 := \mathcal{O}_K^\times$ and $U_K^i := 1 + \mathfrak{m}_K^i$ for $i \geq 1$. The notations U_L^i and k_L are defined in the same way.

1. Show that $U_K^0/U_K^1 \cong k_K^\times$ and $U_K^i/U_K^{i+1} \cong k_K$ for $i \geq 1$ as isomorphisms of groups.
2. Show that the norm map $N_{L/K} : L^\times \to K^\times$ induces surjections: $U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$ for all $i \geq 0$.
3. Show that $N_{L/K}(U_L^i) = U_K^i$ for all $i \geq 0$.

proof of 1. The same proof applies to the field L. We will prove it for K.

Case 1: $i = 0$**.** We want to show $U_K^0/U_K^1 \cong k_K^\times$. Consider the reduction modulo $\mathfrak{m}_K$ map, which is a ring homomorphism $\phi : \mathcal{O}_K \to k_K$. We restrict this to the group of units $\mathcal{O}_K^\times$, which gives a group homomorphism $\phi : \mathcal{O}_K^\times \to k_K^\times$.

- **Surjectivity:** Any element $\bar{a} \in k_K^\times$ can be lifted to an element $a \in \mathcal{O}_K$. Since $\bar{a} \neq 0$, a is not in the maximal ideal $\mathfrak{m}_K$. In the local ring $\mathcal{O}_K$, any element not in the maximal ideal is a unit, so $a \in \mathcal{O}_K^\times$. Then $\phi(a) = \bar{a}$. Thus, the map is surjective.
- **Kernel:** The kernel of ϕ consists of units $u \in \mathcal{O}_K^\times$ such that $\phi(u) = 1 \in k_K^\times$. This means $u \equiv 1 \pmod{\mathfrak{m}_K}$, which is precisely the definition of the group of principal units $U_K^1 = 1 + \mathfrak{m}_K$.

By the First Isomorphism Theorem for groups, $U_K^0/\ker(\phi) \cong \mathrm{im}(\phi)$, which gives $U_K^0/U_K^1 \cong k_K^\times$.

Case 2: $i \geq 1$**.** We want to show $U_K^i/U_K^{i+1} \cong k_K$ as an isomorphism of groups (where the operation on k_K is addition). Let π be a uniformizer for K. An element of $U_K^i = 1 + \mathfrak{m}_K^i$ has the form $1 + \pi^i x$ for some $x \in \mathcal{O}_K$. Define the map $\psi : U_K^i \to k_K$ by $\psi(1 + \pi^i x) = x \pmod{\mathfrak{m}_K}$.

- **Homomorphism:** Let $u = 1 + \pi^i x$ and $v = 1 + \pi^i y$ be two elements in U_K^i. Their product is:
$$uv = (1 + \pi^i x)(1 + \pi^i y) = 1 + \pi^i(x + y) + \pi^{2i} xy$$
Since $i \geq 1$, we have $2i \geq i+1$, which means $\pi^{2i} xy \in \mathfrak{m}_K^{i+1}$. Therefore, $uv \equiv 1+\pi^i(x+y) \pmod{\mathfrak{m}_K^{i+1}}$. Applying the map ψ, we get $\psi(uv) = (x + y) \pmod{\mathfrak{m}_K}$. On the other hand, $\psi(u) + \psi(v) = (x \pmod{\mathfrak{m}_K}) + (y \pmod{\mathfrak{m}_K}) = (x + y) \pmod{\mathfrak{m}_K}$. Thus, $\psi(uv) = \psi(u) + \psi(v)$, and ψ is a group homomorphism.

- **Surjectivity:** For any $\bar{a} \in k_K$, lift it to an element $a \in \mathcal{O}_K$. The element $u = 1 + \pi^i a$ is in U_K^i, and $\psi(u) = a \pmod{\mathfrak{m}_K} = \bar{a}$. The map is surjective.

- **Kernel:** The kernel consists of elements $u = 1+\pi^i x$ such that $\psi(u) = 0$. This condition means $x \pmod{\mathfrak{m}_K} = 0$, so $x \in \mathfrak{m}_K$. An element $x \in \mathfrak{m}_K$ can be written as $x = \pi y$ for some $y \in \mathcal{O}_K$. Then $u = 1 + \pi^i(\pi y) = 1 + \pi^{i+1} y$, which means $u \in 1 + \mathfrak{m}_K^{i+1} = U_K^{i+1}$. So, $\ker(\psi) = U_K^{i+1}$.

By the First Isomorphism Theorem, $U_K^i/\ker(\psi) \cong \mathrm{im}(\psi)$, which gives $U_K^i/U_K^{i+1} \cong k_K$. □

proof of 2. First, we note that $\mathrm{N}_{L/K}$ maps U_L^i to U_K^i. Because L/K is unramified, the uniformizer π of K is also a uniformizer of L. For $x = 1 + y$ with $y \in \mathfrak{m}_L^i$, the norm is $\mathrm{N}_{L/K}(1+y) = 1 + \mathrm{Tr}_{L/K}(y) + \cdots + \mathrm{N}_{L/K}(y)$. Since $y \in \mathfrak{m}_L^i$, all its conjugates are as well, so $\mathrm{Tr}_{L/K}(y) \in \mathfrak{m}_K^i$ and all other terms have higher valuation. Thus $\mathrm{N}_{L/K}(1+y) \in 1+\mathfrak{m}_K^i = U_K^i$. So the norm map induces a group homomorphism $\bar{\mathrm{N}} : U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$.

Case 1: $i = 0$**.** The induced map is $\bar{\mathrm{N}} : U_L^0/U_L^1 \to U_K^0/U_K^1$. Using the isomorphism from part (a), this corresponds to a map $k_L^\times \to k_K^\times$. For an unramified extension, the reduction of the norm is the norm of the reduction. That is, for any $u \in \mathcal{O}_L^\times$, we have $\mathrm{N}_{L/K}(u) \pmod{\mathfrak{m}_K} = \mathrm{N}_{k_L/k_K}(u \pmod{\mathfrak{m}_L})$. This means the induced map is precisely the norm map on the residue fields, $\mathrm{N}_{k_L/k_K} : k_L^\times \to k_K^\times$. The norm map for an extension of finite fields is always surjective.

Case 2: $i \geq 1$**.** The induced map is $\bar{\mathrm{N}} : U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$. Using the isomorphism from part (a), this corresponds to a map $k_L \to k_K$. Let's trace the maps. An element $\bar{a} \in k_L$

is lifted to $a \in \mathcal{O}_L$ and corresponds to $u = 1 + \pi^i a \in U_L^i$. We compute its norm:

$$\mathrm{N}_{L/K}(u) = \mathrm{N}_{L/K}(1 + \pi^i a) = 1 + \mathrm{Tr}_{L/K}(\pi^i a) + \text{higher order terms}$$

Since $\pi^i \in K$, this is $1 + \pi^i \mathrm{Tr}_{L/K}(a) + \dots$. The higher order terms lie in $\mathfrak{m}_K^{i+1}$. Thus, $\mathrm{N}_{L/K}(u) \equiv 1 + \pi^i \mathrm{Tr}_{L/K}(a) \pmod{\mathfrak{m}_K^{i+1}}$. The image of this element in U_K^i/U_K^{i+1} corresponds to the element $\mathrm{Tr}_{L/K}(a) \pmod{\mathfrak{m}_K}$ in k_K. For an unramified extension, the reduction of the trace is the trace of the reduction: $\mathrm{Tr}_{L/K}(a) \pmod{\mathfrak{m}_K} = \mathrm{Tr}_{k_L/k_K}(a \pmod{\mathfrak{m}_L})$. So the induced map is the trace map on residue fields, $\mathrm{Tr}_{k_L/k_K} : k_L \to k_K$. The trace map for an extension of finite fields is always surjective. □

proof of 3. We know that $\mathrm{N}_{L/K}(U_L^i) \subseteq U_K^i$. We need to show the reverse inclusion, $U_K^i \subseteq \mathrm{N}_{L/K}(U_L^i)$. We construct a preimage using an approximation argument that relies on the completeness of the fields.

Let $y \in U_K^i$. We will construct a sequence $(x_j)_{j \geq 0}$ in U_L^i such that:

1. $x_0 = 1$.
2. $x_{j+1} x_j^{-1} \in U_L^{i+j}$.
3. $y \cdot \mathrm{N}_{L/K}(x_j)^{-1} \in U_K^{i+j}$ for all $j \geq 0$.

Base Case ($j = 0$): Let $x_0 = 1$. Then $y \cdot \mathrm{N}_{L/K}(x_0)^{-1} = y \in U_K^i$. The condition holds.

Inductive Step: Assume we have constructed x_j satisfying the conditions. Let $y_j = y \cdot \mathrm{N}_{L/K}(x_j)^{-1} \in U_K^{i+j}$. We want to find a correction factor $u_j \in U_L^{i+j}$ such that if we set $x_{j+1} = x_j u_j$, the conditions are satisfied for $j + 1$.

The condition we need to satisfy is $y \cdot \mathrm{N}_{L/K}(x_{j+1})^{-1} \in U_K^{i+j+1}$.

$$y \cdot \mathrm{N}_{L/K}(x_j u_j)^{-1} = (y \cdot \mathrm{N}_{L/K}(x_j)^{-1}) \cdot \mathrm{N}_{L/K}(u_j)^{-1} = y_j \cdot \mathrm{N}_{L/K}(u_j)^{-1}$$

We need this to be in U_K^{i+j+1}, which is equivalent to $y_j \equiv \mathrm{N}_{L/K}(u_j) \pmod{U_K^{i+j+1}}$.

We have $y_j \in U_K^{i+j}$. From part (b), the map $\mathrm{N}_{L/K} : U_L^{i+j}/U_L^{i+j+1} \to U_K^{i+j}/U_K^{i+j+1}$ is surjective. Therefore, for the element $[y_j] \in U_K^{i+j}/U_K^{i+j+1}$, there exists an element $[u_j] \in U_L^{i+j}/U_L^{i+j+1}$ such that $\mathrm{N}_{L/K}([u_j]) = [y_j]$. Let u_j be a representative of this class in U_L^{i+j}. This u_j satisfies the required congruence. We define $x_{j+1} = x_j u_j$.

Convergence: The sequence is defined by $x_{j+1} = x_j u_j$ where $u_j = 1 + z_j$ for $z_j \in \mathfrak{m}_L^{i+j}$. The sequence of partial products $x_j = \prod_{k=0}^{j-1} u_k$ is a Cauchy sequence in the complete metric space U_L^i. Therefore, the sequence converges to a limit $x = \lim_{j \to \infty} x_j \in U_L^i$.

Since the norm map $\mathrm{N}_{L/K}$ is continuous, we have:

$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{L/K}(\lim_{j\to\infty} x_j) = \lim_{j\to\infty} \mathrm{N}_{L/K}(x_j)$$

From condition (3), $y \cdot \mathrm{N}_{L/K}(x_j)^{-1} \in U_K^{i+j}$. As $j \to \infty$, the groups U_K^{i+j} converge to $\{1\}$ (i.e., any element in U_K^{i+j} approaches 1).

$$\lim_{j\to\infty}(y \cdot \mathrm{N}_{L/K}(x_j)^{-1}) = 1 \implies y \cdot (\lim_{j\to\infty} \mathrm{N}_{L/K}(x_j))^{-1} = 1$$

This implies $y = \lim_{j\to\infty} \mathrm{N}_{L/K}(x_j) = \mathrm{N}_{L/K}(x)$.

We have found an $x \in U_L^i$ such that $\mathrm{N}_{L/K}(x) = y$. This proves that $U_K^i \subseteq \mathrm{N}_{L/K}(U_L^i)$, and therefore $\mathrm{N}_{L/K}(U_L^i) = U_K^i$. □

Homework 6.3. For the projection: $\mathrm{pr} : W_K^{ab} \to \mathbb{Z}$, we fix a group theoretic section $\mathbb{Z} \to W_K^{ab}$ and thereby obtain a group isomorphism $W_K^{ab} \simeq I_K \times \mathbb{Z}$. Equip W_K^{ab} with the topology such that this bijection is a homeomorphism, where $I_K \times \mathbb{Z}$ has the product topology with I_K having the subspace topology inherited from $\mathrm{Gal}(K^{ab}/K)$ and $\mathbb{Z}$ having the discrete topology.

1. Show that the topology on W_K^{ab} doesn't depend on the choice of the section.
2. Show that W_K^{ab} is a topological group.
3. Show that the inclusion map $W_K^{ab} \to \mathrm{Gal}(K^{ab}/K)$ is continuous and has dense image, but it is not a homeomorphism onto the image.

proof of 1. Let s and s' be two different group-theoretic sections from $\mathbb{Z}$ to W_K^{ab}. These define two isomorphisms, $\phi_s : I_K \times \mathbb{Z} \to W_K^{ab}$ and $\phi_{s'} : I_K \times \mathbb{Z} \to W_K^{ab}$. Let $\mathcal{T}_s$ be the topology on W_K^{ab} making ϕ_s a homeomorphism, and $\mathcal{T}_{s'}$ be the topology making $\phi_{s'}$ a homeomorphism. We must show that $\mathcal{T}_s = \mathcal{T}_{s'}$.

This is equivalent to showing that the identity map $\mathrm{id} : (W_K^{ab}, \mathcal{T}_s) \to (W_K^{ab}, \mathcal{T}_{s'})$ is a homeomorphism. This, in turn, is equivalent to showing that the composite map $F = \phi_{s'}^{-1} \circ \phi_s : I_K \times \mathbb{Z} \to I_K \times \mathbb{Z}$ is a homeomorphism.

Let's find the formula for F. Let $\sigma = s(1)$ and $\sigma' = s'(1)$. Since $\mathrm{pr}(\sigma) = \mathrm{pr}(\sigma') = 1$, their quotient $\sigma'\sigma^{-1}$ is in the kernel of pr, which is I_K. Let $i_0 = \sigma'\sigma^{-1} \in I_K$. Then $\sigma' = i_0\sigma$. Since W_K^{ab} is abelian and s, s' are homomorphisms, we have $s'(n) = (\sigma')^n = (i_0\sigma)^n = i_0^n\sigma^n = i_0^n s(n)$.

Now, let's compute $F(i, n)$:

$$\phi_s(i, n) = i \cdot s(n)$$

We need to find $(i', n') = \phi_{s'}^{-1}(i \cdot s(n))$. This means we must solve $i' \cdot s'(n') = i \cdot s(n)$. Applying the projection pr to both sides gives $n' = n$. Substituting this back, we get $i' \cdot s'(n) = i \cdot s(n)$, which gives:

$$i' = i \cdot s(n) \cdot s'(n)^{-1} = i \cdot s(n) \cdot (i_0^n s(n))^{-1} = i \cdot s(n) \cdot s(n)^{-1} \cdot i_0^{-n} = i \cdot i_0^{-n}$$

So the map is $F(i, n) = (i \cdot i_0^{-n}, n)$.

We must check that F is a homeomorphism.

- **Continuity of** F: The second component map $(i, n) \mapsto n$ is continuous. The first component map is $(i, n) \mapsto i \cdot i_0^{-n}$. The map $n \mapsto i_0^{-n}$ from $\mathbb{Z}$ to I_K is continuous because $\mathbb{Z}$ has the discrete topology. The map $(i, n) \mapsto i$ is continuous (projection). Since I_K is a topological group, its multiplication is continuous. Thus, the map $(i, n) \mapsto i \cdot i_0^{-n}$ is a composition of continuous maps, and is therefore continuous. Since both components are continuous, F is continuous.

- **Continuity of** F^{-1}: We find the inverse map. If $(i', n') = F(i, n)$, then $n' = n$ and $i' = i \cdot i_0^{-n}$, so $i = i' \cdot i_0^n = i' \cdot i_0^{n'}$. Thus, $F^{-1}(i', n') = (i' \cdot i_0^{n'}, n')$. This map has the same form as F, and is continuous by the same reasoning.

Since F is a homeomorphism, the two topologies $\mathcal{T}_s$ and $\mathcal{T}_{s'}$ are identical. □

proof of 2. We need to show that the group multiplication and inversion maps on W_K^{ab} are continuous with respect to the defined topology. We can check this on the model space $I_K \times \mathbb{Z}$, using the isomorphism ϕ_s.

Multiplication: Let (i_1, n_1) and (i_2, n_2) be two elements in $I_K \times \mathbb{Z}$. Their product in W_K^{ab} is:

$$\phi_s(i_1, n_1) \cdot \phi_s(i_2, n_2) = (i_1 \cdot s(n_1)) \cdot (i_2 \cdot s(n_2))$$

Since W_K^{ab} is abelian and s is a homomorphism:

$$= (i_1 \cdot i_2) \cdot (s(n_1) \cdot s(n_2)) = (i_1 \cdot i_2) \cdot s(n_1 + n_2)$$

This element is $\phi_s(i_1 \cdot i_2, n_1 + n_2)$. So, the multiplication map on $I_K \times \mathbb{Z}$ is $m((i_1, n_1), (i_2, n_2)) = (i_1 \cdot i_2, n_1 + n_2)$. This map is continuous because the component maps (multiplication in I_K and addition in $\mathbb{Z}$) are continuous for their respective topological groups.

Inversion: Let $(i, n) \in I_K \times \mathbb{Z}$. The inverse of $\phi_s(i, n) = i \cdot s(n)$ is:

$$(i \cdot s(n))^{-1} = s(n)^{-1} \cdot i^{-1} = s(-n) \cdot i^{-1} = i^{-1} \cdot s(-n)$$

This element is $\phi_s(i^{-1}, -n)$. So, the inversion map on $I_K \times \mathbb{Z}$ is $\text{inv}(i, n) = (i^{-1}, -n)$. This map is continuous because the component maps (inversion in I_K and negation in $\mathbb{Z}$) are continuous.

Since both multiplication and inversion are continuous, W_K^{ab} is a topological group.

□

proof of 3. Let $j : W_K^{ab} \to \text{Gal}(K^{ab}/K)$ be the canonical inclusion map from local class field theory. First note that $\text{pr} : \text{Gal}(K^{ab}/K) \to \text{Gal}(K^{ur}/K)$ is a quotient map, therefore is an open continuous map. Denote the section by $s : \mathbb{Z} \to \text{Gal}(K^{ab}/K)$, where $s(1) = \sigma$.

- **Continuity:**

For any element $\tau = j(i, n) = i \cdot \sigma^n$ in $\text{Gal}(K^{ab}/K)$ and its neighborhood U, our goal is to find a neighborhood $V_1 \times V_2$ of (i, n) in W_K^{ab} such that $j(V_1 \times V_2) \subseteq U$. Because $\mathbb{Z}$ is equipped with the discrete topology, we can choose $V_2 = \{n\}$. Then choose $V_1 = U \cdot \sigma^{-n} \cap I_K$.

- **Dense Image:**

For any element τ in $\text{Gal}(K^{ab}/K)$ and its neighborhood U, our goal is to prove $U \cap W_K^{ab} \neq \emptyset$. $\text{pr}(U)$ is open in $\text{Gal}(K^{ur}/K) \simeq \hat{\mathbb{Z}}$. Since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$, there exists an integer $n \in \mathbb{Z}$ such that $n \in \text{pr}(U)$, i.e. there exists an element $\tau' \in U$ such that $\text{pr}(\tau') = n$. Then $\tau' \in U \cap W_K^{ab}$.

- **Not a Homeomorphism:** (**Remark:** This is just: the product topology on W_K^{ab} is not the subspace topology inherited from $\text{Gal}(K^{ab}/K)$.)

Consider $I_K \times \{0\} \subseteq I_K \times \mathbb{Z} \Leftrightarrow I_K \subset W_K^{ab}$. In the product topology on W_K^{ab}, $I_K \times \{0\}$ is a open subset since $\{0\}$ is open in the discrete topology on $\mathbb{Z}$.

Suppose in the subspace topology inherited from W_K^{ab}, I_K is also open. Then there exists an open subset U in $\text{Gal}(K^{ab}/K)$ such that $U \cap W_K^{ab} = I_K$.

$\text{pr}(U)$ is open in $\text{Gal}(K^{ur}/K) \simeq \hat{\mathbb{Z}}$. Since

(i) $\hat{\mathbb{Z}}$ is not discrete.

(ii) $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$.

(iii) $\hat{\mathbb{Z}}$ is profinite therefore Hausdorff.

It is easy to show that any non-empty open subset of $\hat{\mathbb{Z}}$ contains infinitely many integers. Thus, $\text{pr}(U)$ contains an integer $n \neq 0$.

Therefore there exists an element $\tau \in U$ such that $\text{pr}(\tau) = n \neq 0$. Then $\tau \in U \cap W_K^{ab}$. This is a contradiction since $U \cap W_K^{ab} = I_K$ and $\text{pr}(I_K) = 0$. □

7 2025.10.23

Corollary 7.1 (**Norm Functoriality**)**.** For a finite abelian extension L/K, the following diagram commutes:

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ K^* & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

Proposition 7.1 (**Transfer Functoriality**)**.** For a finite abelian extension L/K, the following diagram commutes, where i is the inclusion map and Ver is the transfer map (Verlagerung).

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^* & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

Theorem 7.1 (**Local-Global Compatibility**)**.** For a number field K and any place v of K, the following diagram commutes. Here C_K denotes the idele class group of K.

$$\begin{array}{ccc} K_v^* & \xrightarrow{\psi_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

Remark: We will use local-global compatibility to glue the global Artin map from the local Artin maps.

7.1 Ideal-theoretic Formulation of Global Class Field Theory

Definition 7.1. A **modulus** $\mathfrak{m}$ in a number field K is a formal expression

$$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$$

where $\mathfrak{m}_0 \subseteq \mathcal{O}_K$ is a non-zero integral ideal, and $\mathfrak{m}_\infty$ is a subset of the real places of K.

Definition 7.2. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus in K. We define a subgroup $U_\mathfrak{m}$ of the idele group $\mathbb{A}_K^\times$ as

$$U_\mathfrak{m} := \prod_{v \in V_{K,f}} U_{\mathfrak{m},v} \times \prod_{v \in V_{K,\infty}} U_{\mathfrak{m},v}$$

where the local components are defined as follows:

- For a finite place v corresponding to the prime ideal $\mathfrak{p}_v$, let $e_v = \mathrm{ord}_{\mathfrak{p}_v}(\mathfrak{m}_0)$. Then

$$U_{\mathfrak{m},v} = U_{K_v}^{(e_v)} := \begin{cases} 1 + \mathfrak{m}_{K_v}^{e_v}\mathcal{O}_{K_v} & \text{if } e_v > 0 \\ \mathcal{O}_{K_v}^\times & \text{if } e_v = 0 \end{cases}$$

- For an infinite place v,

$$U_{\mathfrak{m},v} := \begin{cases} \mathbb{R}_{>0}^\times & \text{if } v \in \mathfrak{m}_\infty \text{ (real)} \\ K_v^\times & \text{if } v \notin \mathfrak{m}_\infty \text{ (real or complex)} \end{cases}$$

Exercise 7.1. Every open subgroup of $\mathbb{I}_K$ contains $U_\mathfrak{m}$ for some modulus $\mathfrak{m}$.

Let $\overline{U}_\mathfrak{m}$ be the image of $U_\mathfrak{m}$ via the canonical projection $\mathbb{I}_K \to C_K$. Then $\overline{U}_\mathfrak{m}$ is an open subgroup of C_K.

Fact: The set of subgroups $\{\overline{U}_\mathfrak{m}\}_\mathfrak{m}$ forms a cofinal system of open subgroups of C_K.

Recall: There is an inclusion-reversing bijection between the set of open subgroups of C_K and the set of finite abelian extensions of K.

$$\begin{array}{ccc} \{\text{open subgroups of } C_K\} & \longleftrightarrow & \{\text{finite abelian extensions of } K\} \\ N_{L/K}(C_L) & \mapsto & L \\ \overline{U}_\mathfrak{m} & \hookleftarrow & K_\mathfrak{m} \end{array}$$

Definition 7.3. The finite abelian extension $K_\mathfrak{m}/K$ corresponding to the open subgroup $\overline{U}_\mathfrak{m} \subseteq C_K$ is called the **ray class field** corresponding to the modulus $\mathfrak{m}$. Then the Artin map induces an isomorphism:

$$\psi_K : C_K/\overline{U}_\mathfrak{m} \xrightarrow{\sim} \mathrm{Gal}(K_\mathfrak{m}/K)$$

Corollary 7.2 (**Abstract Kronecker-Weber Theorem**). The maximal abelian extension of K is the union of all ray class fields:

$$K^{\mathrm{ab}} = \bigcup_{\mathfrak{m}} K_{\mathfrak{m}}$$

Exercise 7.2. For $K = \mathbb{Q}$:

1. Let $\mathfrak{m} = (m)\infty$ with $m \in \mathbb{Z}_{\geq 1}$. Then the ray class field corresponding to $\mathfrak{m}$ is $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity.
2. Determine the ray class field for the modulus $\mathfrak{m} = (m)$ (Note: in this case $\mathfrak{m}_\infty = \emptyset$).

This recovers the Kronecker-Weber theorem for $\mathbb{Q}$.

Goal: Relate $C_K/\overline{U}_{\mathfrak{m}}$ to class groups.

Definition 7.4. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus for a number field K.

1. The group of fractional ideals of K prime to $\mathfrak{m}_0$, denoted by $\mathcal{I}_K^{(\mathfrak{m})}$, is the subgroup of fractional ideals whose prime factorization contains no prime ideals that divide $\mathfrak{m}_0$.

$$\begin{aligned}\mathcal{I}_K^{(\mathfrak{m})} &= \{\mathfrak{a} \text{ is a fractional ideal} \mid \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all prime ideals } \mathfrak{p} \text{ dividing } \mathfrak{m}_0\} \\ &\cong \bigoplus_{\mathfrak{p} \nmid \mathfrak{m}_0} \mathbb{Z} \cdot \mathfrak{p}\end{aligned}$$

   This is the free abelian group generated by the prime ideals of K not dividing $\mathfrak{m}_0$.

2. We define the subgroup $K^\times_{(\mathfrak{m})}$ of the multiplicative group $K^\times$ as:

$$K^\times_{(\mathfrak{m})} := \left\{ x \in K^\times \;\middle|\; \begin{array}{ll} x_v > 0 & \text{for all real places } v \in \mathfrak{m}_\infty \\ x \equiv 1 & (\mathrm{mod}\ \mathfrak{m}_0) \end{array} \right\}$$

   The congruence $x \equiv 1 \pmod{\mathfrak{m}_0}$ means that for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}_0$, if $e_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$, then $\mathrm{ord}_{\mathfrak{p}}(x-1) \geq e_{\mathfrak{p}}$, which also means $x \in U_{K_v}^{e_v}$ for all $v \in V_{K,f}$ such that $\mathfrak{p}_v | \mathfrak{m}_0$. From now on, we will simply write $v \mid \mathfrak{m}_0$.

There is a natural group homomorphism from $K^\times_{(\mathfrak{m})}$ to $\mathcal{I}_K^{(\mathfrak{m})}$ given by mapping an element

x to the principal fractional ideal (x) it generates.

$$\begin{aligned} K_{(\mathfrak{m})}^{\times} &\longrightarrow \mathcal{I}_K^{(\mathfrak{m})} \\ x &\longmapsto (x) \end{aligned}$$

Definition 7.5. The **ray class group** modulo $\mathfrak{m}$ is defined as the cokernel of the above homomorphism:

$$\mathrm{Cl}_{\mathfrak{m}}(K) := \mathrm{coker}\left(K_{(\mathfrak{m})}^{\times} \to \mathcal{I}_K^{(\mathfrak{m})}\right) = \frac{\mathcal{I}_K^{(\mathfrak{m})}}{\{(x) \mid x \in K_{(\mathfrak{m})}^{\times}\}}$$

Example 7.1.

1. Let $\mathfrak{m} = (1)$ be the trivial modulus. This corresponds to $\mathfrak{m}_0 = \mathcal{O}_K$ and $\mathfrak{m}_\infty = \emptyset$. In this case, $\mathcal{I}_K^{(\mathfrak{m})}$ is the group of all fractional ideals $\mathcal{I}_K$, and $K_{(\mathfrak{m})}^{\times} = K^{\times}$. The ray class group is then the ordinary ideal class group of K:

$$\mathrm{Cl}_{\mathfrak{m}}(K) = \frac{\mathcal{I}_K}{\{(x) \mid x \in K^{\times}\}} = \mathrm{Cl}(K)$$

2. Let $\mathfrak{m}_+ = (1)\mathfrak{m}_\infty$, where $\mathfrak{m}_\infty$ consists of all real places of K. The corresponding ray class group $\mathrm{Cl}_{\mathfrak{m}_+}(K)$ is called the **narrow class group** of K, and is often denoted by $\mathrm{Cl}^+(K)$. We will have a natural surjective homomorphism from the narrow class group to the ordinary class group:

$$\mathrm{Cl}^+(K) \twoheadrightarrow \mathrm{Cl}(K)$$

Example 7.2. Compute the ray class group of $K = \mathbb{Q}$ for the modulus $\mathfrak{m} = (m)\infty$ and (m) with $m \in \mathbb{Z}_{\geq 1}$.

The groups of fractional ideals prime to (m) and $(m)\infty$ are both:

$$\mathcal{I}_{\mathbb{Q}}^{((m))} = \mathcal{I}_{\mathbb{Q}}^{((m)\infty)} = \left\{\frac{a}{b} \in \mathbb{Q}^{\times} \mid (a, m) = 1 = (b, m)\right\}.$$

- For $\mathfrak{m} = (m)\infty$: The subgroup of principal ideals is given by

$$\mathbb{Q}_{(\mathfrak{m})}^{\times} = \left\{\frac{a}{b} \in \mathbb{Q}_{>0}^{\times} \mid a \cdot b^{-1} \equiv 1 \pmod{m}\right\}.$$

There is a natural group homomorphism:

$$\begin{aligned} \mathcal{I}_{\mathbb{Q}}^{(\mathfrak{m})} &\longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times} \\ \frac{a}{b} &\longmapsto a \cdot b^{-1} \pmod{m} \end{aligned}$$

This map is surjective, and its kernel is the set of principal ideals generated by elements of $\mathbb{Q}_{(\mathfrak{m})}^{\times}$. This gives an isomorphism for the ray class group:

$$\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

- For $\mathfrak{m} = (m)$: The subgroup of principal ideals is given by

$$\mathbb{Q}_{(\mathfrak{m})}^{\times} = \left\{ \frac{a}{b} \in \mathbb{Q}^{\times} \mid a \cdot b^{-1} \equiv 1 \pmod{m} \right\}.$$

The homomorphism from $\mathbb{Q}_{(\mathfrak{m})}^{\times}$ to $\mathcal{I}_{\mathbb{Q}}^{(\mathfrak{m})}$ is exactly:

$$\begin{aligned} \mathbb{Q}_{(\mathfrak{m})}^{\times} &\longrightarrow \mathcal{I}_{\mathbb{Q}}^{(\mathfrak{m})} \\ \frac{a}{b} &\longmapsto \left|\frac{a}{b}\right| \end{aligned}$$

This leads to the isomorphism:

$$\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}/\{\pm 1\}$$

Proposition 7.2. For any modulus $\mathfrak{m}$, there is a canonical isomorphism of groups

$$C_K/\overline{U}_{\mathfrak{m}} \cong \mathrm{Cl}_{\mathfrak{m}}(K).$$

Remark: $K^{\times} \cap U_{\mathfrak{m}} \neq K_{\mathfrak{m}}^{\times}$

Proof. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_{\infty}$ be a modulus. Let $\mathbb{I}_{K,\mathfrak{m}}$ be the subgroup of the idele group $\mathbb{I}_K$ defined by

$$\mathbb{I}_{K,\mathfrak{m}} := \left\{ (x_v) \in \mathbb{I}_K \mid x_v \in \mathbb{R}_{>0} \text{ for } v \in \mathfrak{m}_{\infty}, \text{ and } x_v \in U_{K_v}^{(e_v)} \text{ for } v \mid \mathfrak{m}_0 \right\}.$$

From the definitions, we have the crucial identity $K^{\times} \cap \mathbb{I}_{K,\mathfrak{m}} = K_{(\mathfrak{m})}^{\times}$.

Consider the quotient group $\mathbb{I}_{K,\mathfrak{m}}/U_{\mathfrak{m}}$. The local components are:

- For $v \in \mathfrak{m}_{\infty}$ or $v \mid \mathfrak{m}_0$, the component is trivial.
- For a finite place $v \nmid \mathfrak{m}_0$, the component is $K_v^{\times}/\mathcal{O}_{K_v}^{\times} \cong \mathbb{Z}$ via the valuation map ord_v.

This gives a canonical isomorphism:

$$\mathbb{I}_{K,\mathfrak{m}}/U_{\mathfrak{m}} \xrightarrow{\sim} \bigoplus_{v\nmid\mathfrak{m}_0, v\in V_{K,f}} \mathbb{Z} \cong \mathcal{I}_K^{(\mathfrak{m})}.$$

The argument can be summarized by the following commutative diagram and isomorphisms:

$$\begin{array}{ccc} \mathbb{I}_{K,\mathfrak{m}}/U_{\mathfrak{m}} & \xrightarrow{\quad\sim\quad} & \mathcal{I}_K^{(\mathfrak{m})} \\ \downarrow & & \downarrow \\ \mathbb{I}_{K,\mathfrak{m}}/(K^\times_{(\mathfrak{m})}U_{\mathfrak{m}}) & \xrightarrow{\sim} & \mathrm{Cl}_{\mathfrak{m}}(K) \\ \text{need to prove}\updownarrow & & \\ \mathbb{I}_K/(K^\times U_{\mathfrak{m}}) & & \end{array}$$

The right vertical arrow is the definition of the ray class group. The bottom group is $C_K/\overline{U}_{\mathfrak{m}}$.

It suffices to show that the natural map $\phi : \mathbb{I}_{K,\mathfrak{m}} \to \mathbb{I}_K/(K^\times U_{\mathfrak{m}})$ induces an isomorphism

$$\mathbb{I}_{K,\mathfrak{m}}/(K^\times_{(\mathfrak{m})}U_{\mathfrak{m}}) \xrightarrow{\sim} \mathbb{I}_K/(K^\times U_{\mathfrak{m}}).$$

- **Injectivity:**

The kernel of ϕ is $\mathbb{I}_{K,\mathfrak{m}} \cap (K^\times U_{\mathfrak{m}})$. Let $x = ku \in \ker(\phi)$ where $k \in K^\times$ and $u \in U_{\mathfrak{m}}$. Since $U_{\mathfrak{m}} \subset \mathbb{I}_{K,\mathfrak{m}}$, we have $u \in \mathbb{I}_{K,\mathfrak{m}}$. Then $k = xu^{-1}$ must also be in $\mathbb{I}_{K,\mathfrak{m}}$. Thus, $k \in K^\times \cap \mathbb{I}_{K,\mathfrak{m}} = K^\times_{(\mathfrak{m})}$. This shows $\ker(\phi) = K^\times_{(\mathfrak{m})}U_{\mathfrak{m}}$, so the induced map is injective.

- **Surjectivity:**

Let S be the finite set of places of K given by

$$S := V_{K,\infty} \cup \{v \in V_{K,f} : v \mid \mathfrak{m}_0\}.$$

Let $\mathbb{I}_K^S$ be the subgroup of ideles whose components are 1 at the places of S:

$$\mathbb{I}_K^S := \{(x_v) \in \mathbb{I}_K \mid x_v = 1 \text{ for all } v \in S\}.$$

Obviously, we have $\mathbb{I}_K^S \subseteq \mathbb{I}_{K,\mathfrak{m}}$.

Recall: The image of the natural inclusion $\mathbb{I}_K^S \hookrightarrow \mathbb{I}_K \to C_K$ is dense.

It follows that the image of the composite map $\mathbb{I}_K^S \to C_K \to C_K/\overline{U}_{\mathfrak{m}}$ is also dense. However, since $C_K/\overline{U}_{\mathfrak{m}}$ is a finite group and it has the discrete topology, a dense subset of a discrete space must be the entire space. Therefore, the map $\mathbb{I}_K^S \to C_K/\overline{U}_{\mathfrak{m}}$ is surjective. So the map $\mathbb{I}_{K,\mathfrak{m}} \to C_K/\overline{U}_{\mathfrak{m}}$ is also surjective. □

Remark: The surjectivity means that for any idele $x \in \mathbb{I}_K$, there exists an idele $y \in \mathbb{I}_K^S$ such that the class of x is equal to the class of y in $C_K/\overline{U}_{\mathfrak{m}}$.

Corollary 7.3. The ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ is finite for any modulus $\mathfrak{m}$.

Definition 7.6. For any two moduli $\mathfrak{m}$ and $\mathfrak{m}'$, we write $\mathfrak{m} \mid \mathfrak{m}'$ if $\mathfrak{m}_0 \mid \mathfrak{m}'_0$ (which means $\mathfrak{m}'_0 \subseteq \mathfrak{m}_0$ as ideals) and $\mathfrak{m}_\infty \subseteq \mathfrak{m}'_\infty$. We can also define the greatest common divisor of two moduli, $\mathfrak{n} = \gcd(\mathfrak{m}, \mathfrak{m}')$, by setting $\mathfrak{n}_0 = \gcd(\mathfrak{m}_0, \mathfrak{m}'_0) = \mathfrak{m}_0 + \mathfrak{m}'_0$ and $\mathfrak{n}_\infty = \mathfrak{m}_\infty \cap \mathfrak{m}'_\infty$.

Remark: If $\mathfrak{m} \mid \mathfrak{m}'$, then we have inclusions $\mathcal{I}_K^{(\mathfrak{m}')} \subseteq \mathcal{I}_K^{(\mathfrak{m})}$ and $K^\times_{(\mathfrak{m}')} \subseteq K^\times_{(\mathfrak{m})}$. These inclusions induce a natural group homomorphism

$$\mathrm{Cl}_{\mathfrak{m}'}(K) \longrightarrow \mathrm{Cl}_{\mathfrak{m}}(K).$$

This homomorphism is surjective.

proof of remark. Indeed, this follows from the commutativity of the following diagram, where the bottom horizontal map is surjective because the condition $\mathfrak{m} \mid \mathfrak{m}'$ implies $U_{\mathfrak{m}'} \subseteq U_{\mathfrak{m}}$.

$$\begin{array}{ccc} \mathrm{Cl}_{\mathfrak{m}'}(K) & \xrightarrow{\text{surj.}} & \mathrm{Cl}_{\mathfrak{m}}(K) \\ \downarrow \wr & & \downarrow \wr \\ C_K/\overline{U}_{\mathfrak{m}'} & \xrightarrow{\text{surj.}} & C_K/\overline{U}_{\mathfrak{m}} \end{array}$$

□

Recall: We have the following fundamental isomorphisms from class field theory. Let $\psi_{K_{\mathfrak{m}}/K}$ also denote the Artin map from the ray class group:

$$\begin{array}{ccc} C_K/\overline{U}_{\mathfrak{m}} & \xrightarrow[\sim]{\psi_{K_{\mathfrak{m}}/K}} & \mathrm{Gal}(K_{\mathfrak{m}}/K) \\ \wr \uparrow & \nearrow_{\sim} & \\ \mathrm{Cl}_{\mathfrak{m}}(K) & & \end{array}$$

Question:

1. Study the properties of the ray class fields $K_{\mathfrak{m}}$.
2. Study all finite abelian extensions of K using ray class fields. (Any such extension L is contained in $K_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$).

Corollary 7.4. The ray class fields have the following properties:

1. If $\mathfrak{m} \mid \mathfrak{m}'$, then $K_{\mathfrak{m}} \subseteq K_{\mathfrak{m}'}$. We have the following commutative diagram, where the right vertical map is restriction.

$$\begin{array}{ccc} \mathrm{Cl}_{\mathfrak{m}'}(K) & \xrightarrow{\psi_{K_{\mathfrak{m}'}/K}} & \mathrm{Gal}(K_{\mathfrak{m}'}/K) \\ \downarrow & & \downarrow \mathrm{res} \\ \mathrm{Cl}_{\mathfrak{m}}(K) & \xrightarrow{\psi_{K_{\mathfrak{m}}/K}} & \mathrm{Gal}(K_{\mathfrak{m}}/K) \end{array}$$

2. $K_{\mathfrak{m}} \cap K_{\mathfrak{m}'} = K_{\gcd(\mathfrak{m},\mathfrak{m}')}$.

3. A place $v \in V_K$ is unramified in the extension $K_{\mathfrak{m}}/K$ if and only if v does not divide the modulus $\mathfrak{m}$. **Recall:** We say $v \mid \mathfrak{m}$ if:

   - $v \mid \mathfrak{m}_0$ (i.e., $\mathfrak{p}_v \mid \mathfrak{m}_0$) when $v \in V_{K,f}$.
   - $v \in \mathfrak{m}_\infty$ when $v \in V_{K,\infty}$.

Proof of (1). The condition $\mathfrak{m} \mid \mathfrak{m}'$ implies $U_{\mathfrak{m}'} \subseteq U_{\mathfrak{m}}$ by definition. Taking their images in the idele class group, we get $\overline{U}_{\mathfrak{m}'} \subseteq \overline{U}_{\mathfrak{m}}$. By the inclusion-reversing property of the global Artin map correspondence, this implies a reverse inclusion of the corresponding class fields: $K_{\mathfrak{m}'} \supseteq K_{\mathfrak{m}}$.

The commutativity of the diagram follows from the following commutative diagram:

$$\begin{array}{ccccc} \mathrm{Cl}_{\mathfrak{m}'}(K) & \xrightarrow{\simeq} & C_K/\overline{U}_{\mathfrak{m}'} & \xrightarrow{\simeq} & \mathrm{Gal}(K_{\mathfrak{m}'}/K) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Cl}_{\mathfrak{m}}(K) & \xrightarrow{\simeq} & C_K/\overline{U}_{\mathfrak{m}} & \xrightarrow{\simeq} & \mathrm{Gal}(K_{\mathfrak{m}}/K) \end{array}$$

□

Proof of (2). We want to show $K_{\mathfrak{m}} \cap K_{\mathfrak{m}'} = K_{\gcd(\mathfrak{m},\mathfrak{m}')}$. From the fundamental correspondence of class field theory:

$$\begin{array}{ccc} \{\text{open subgroups of } C_K\} & \longleftrightarrow & \{\text{finite abelian extensions of } K\} \\ \overline{U}_{\mathfrak{m}} & \longleftrightarrow & K_{\mathfrak{m}} \\ \overline{U}_{\mathfrak{m}'} & \longleftrightarrow & K_{\mathfrak{m}'} \end{array}$$

The intersection of fields corresponds to the product of the corresponding subgroups. Thus, the field $K_{\mathfrak{m}} \cap K_{\mathfrak{m}'}$ corresponds to the subgroup $\overline{U}_{\mathfrak{m}} \cdot \overline{U}_{\mathfrak{m}'}$. It suffices to show that $U_{\mathfrak{m}} \cdot U_{\mathfrak{m}'} =$

$U_{\gcd(\mathfrak{m},\mathfrak{m}')}$ as subgroups of the idele group $\mathbb{I}_K$. This can be verified easily by checking each local component. □

Proof of (3). From the **Theorem 5.3 (2)**, a place $v \in V_K$ is unramified in $K_\mathfrak{m}/K$ if and only if in the following map:

$$f_v : K_v^\times \xrightarrow{\iota} C_K \xrightarrow{\psi_{K_\mathfrak{m}/K}} \mathrm{Gal}(K_\mathfrak{m}/K)$$

we have

(i) $\mathcal{O}_{K_v}^\times \subseteq \ker(f_v)$ if $v \in V_{K,f}$.

(ii) f_v is trivial if $v \in V_{K,\infty}$.

Hence also if and only if:

(i) $\iota(\mathcal{O}_{K_v}^\times) \subseteq \overline{U}_\mathfrak{m}$ if $v \in V_{K,f}$.

(ii) $\iota(K_v^\times) \subseteq \overline{U}_\mathfrak{m}$ if $v \in V_{K,\infty}$.

By inspecting the definition of the subgroup $U_\mathfrak{m}$,

$$U_\mathfrak{m} = \prod_{u\in V_{K,\infty}, u\notin \mathfrak{m}_\infty} K_u^\times \times \prod_{u\in \mathfrak{m}_\infty} \mathbb{R}_{>0}^\times \times \prod_{u\in V_{K,f}, u\nmid \mathfrak{m}_0} \mathcal{O}_{K_u}^\times \times \prod_{u\mid \mathfrak{m}_0} U_{K_u}^{(e_u)},$$

It is clear that the above two conditions are satisfied if and only if $v \nmid \mathfrak{m}$. □

Definition 7.7. Let L/K be a finite abelian extension.

1. A modulus $\mathfrak{m}$ is said to be **admissible** for L/K if the extension L is contained in the ray class field $K_\mathfrak{m}$.
2. By the theory of class fields, there exists a unique minimal modulus (under the divisibility relation) that is admissible for L/K. This modulus is called the **conductor** of the extension, denoted by $\mathfrak{f}_{L/K}$.

Fact: If a finite abelian extension L is contained in two ray class fields, $K_\mathfrak{m}$ and $K_{\mathfrak{m}'}$, then it is also contained in their intersection, $K_\mathfrak{m} \cap K_{\mathfrak{m}'} = K_{\gcd(\mathfrak{m},\mathfrak{m}')}$. This ensures the existence and uniqueness of the conductor.

Proposition 7.3 (**Conductor-Ramification Theorem**)**.** Let L/K be a finite abelian extension and let v be a place of K. Then v is ramified in L if and only if v divides the conductor $\mathfrak{f}_{L/K}$.

Proof. $\mathfrak{f} := \mathfrak{f}_{L/K}$, then $L \subseteq K_{\mathfrak{f}}$.

"⇒" is easy: if v is ramified in L, then it is also ramified in $K_{\mathfrak{f}}$ by the transitivity of ramification. By **Corollary 7.4(3)**, v must divide $\mathfrak{f} = \mathfrak{f}_{L/K}$.

"⇐": We prove it by contradiction. If v is unramified in L, our goal is to find a modulus $\mathfrak{m}$ such that $\mathfrak{f} \mid \mathfrak{m}$ and $v \nmid \mathfrak{m}$.

Since v is unramified in L, it is well-known that for any $w \in V_L$ such that $w \mid v$,

$$\mathcal{O}_{K_v}^{\times} \subseteq \mathrm{N}_{L_w/K_v}(L_w^{\times})$$

So for the embedding $\iota : K_v^{\times} \hookrightarrow \mathbb{I}_K$, we have

$$\iota(\mathcal{O}_{K_v}^{\times}) \subseteq \mathrm{Im}(\mathrm{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K)$$

So there exists a modulus $\mathfrak{m}$ such that $v \nmid \mathfrak{m}$ and:

$$U_{\mathfrak{m}} \subseteq \mathrm{Im}(\mathrm{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K)$$

From the **Classification of Finite Abelian Extensions (Global Version)**, we have:

$$L \subseteq K_{\mathfrak{m}}$$

So $\mathfrak{f} \mid \mathfrak{m}$ by the definition of conductor. □

7.2 Homework

Homework 7.1. Every open subgroup of $\mathbb{I}_K$ contains $U_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.

Proof. Every open subgroup U of $\mathbb{I}_K$ is of the form:

$$\prod_{v\in\{\text{real places}\}} U_v \times \prod_{v\in\{\text{complex places}\}} U_v \times \prod_{v\in T} U_v \times \prod_{v\in V_{K,f}\setminus T} \mathcal{O}_{K_v}^*$$

where

$$T := \{v \in V_{K,f} | U_v \neq \mathcal{O}_{K,v}^*\}$$

is a finite set of $V_{K,f}$.

Then it is well known that:

- For all real places v, U_v is a open subgroup of $\mathbb{R}^*$, so it must be $\mathbb{R}_{>0}$ or $\mathbb{R}^*$.
- For all complex places v, U_v is a open subgroup of $\mathbb{C}^*$, so it must be $\mathbb{C}^*$.
- For each finite place $v \in T$, since U_v is an open subgroup of K_v^*, hence a neighbourhood of 1. So there exists an integer $e_v \geq 0$ such that

$$1 + \mathfrak{m}_{K_v}^{e_v} \subseteq U_v$$

Consider the modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$:

$$\mathfrak{m}_0 := \prod_{v\in T} \mathfrak{p}_v^{e_v}$$
$$\mathfrak{m}_\infty := \{v \in V_{K,\infty} | U_v = \mathbb{R}_{>0}\}$$

Obviously we have $U_{\mathfrak{m}} \subseteq U$. □

Homework 7.2. Let $K = \mathbb{Q}$.

(a) Let $\mathfrak{m} = m\infty$ be a modulus of $\mathbb{Q}$ with $m \in \mathbb{Z}_{\geq 1}$. Show that the ray class field corresponding to $\mathfrak{m}$ is $\mathbb{Q}(\zeta_m)$;

(b) Determine also the ray class field corresponding to $\mathfrak{m} = m$ (with $\mathfrak{m}_\infty = \emptyset$);

(c) Compute the conductor of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ for any square free $d \in \mathbb{Z}$;

(d) Compute the conductor of $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}$.

Prove of (a). (**Remark:** The proof is obtained from Neukirch's *Algebraic Number Theory*)

Lemma 7.1. The group of norms of the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is the group $(p) \times U^{(n)}_{\mathbb{Q}_p}$.

Proof of Lemma. Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_{p^n})$. It is well-known that the extension L/K is totally ramified of degree $\varphi(p^n) = p^{n-1}(p-1)$, and if ζ is a primitive p^n-th root of unity, then $1-\zeta$ is a prime element of L of norm $\mathrm{N}_{L/K}(1-\zeta) = p$.

We now consider the exponential map of $\mathbb{Q}_p$. It gives an isomorphism

$$\exp : \mathfrak{p}_K^{\nu} \to U_K^{(\nu)}$$

for $\nu \geq 1$, provided $p \neq 2$, and for $\nu \geq 2$, even if $p = 2$.

It transforms the isomorphism $\mathfrak{p}_K^{\nu} \to \mathfrak{p}_K^{\nu+s-1}$ given by $a \mapsto p^{s-1}(p-1)a$, into the isomorphism $U_K^{(\nu)} \to U_K^{(\nu+s-1)}$ given by $x \mapsto x^{p^{s-1}(p-1)}$, so that $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$ if $p \neq 2$, and $(U_K^{(2)})^{2^{n-2}} = U_K^{(n)}$ if $p = 2, n > 1$ (the case $p = 2, n = 1$ is trivial).

Consequently, we have $U_K^{(n)} \subseteq \mathrm{N}_{L/K}(L^*)$ if $p \neq 2$. For $p = 2$ we note that

$$U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(2)})^2 \cup 5(U_K^{(2)})^2$$

because a number that is congruent to 1 mod 4 is congruent to 1 or 5 mod 8. Hence

$$U_K^{(n)} = (U_K^{(2)})^{2^{n-1}} \cup 5^{2^{n-2}}(U_K^{(2)})^{2^{n-1}}.$$

It is easy to show that $5^{2^{n-2}} = \mathrm{N}_{L/K}(2+i)$, so $U_K^{(n)} \subseteq \mathrm{N}_{L/K}L^*$ holds also in case $p = 2$. Since $p = \mathrm{N}_{L/K}(1-\zeta)$, we have $(p) \times U_K^{(n)} \subseteq \mathrm{N}_{L/K}L^*$, and since both groups have index $p^{n-1}(p-1)$ in K^*, we do find that $\mathrm{N}_{L/K}L^* = (p) \times U_K^{(n)}$ as claimed. □

Back to the proof of (a):

Let $m = \prod_{p \neq p_\infty} p^{n_p}$. Then $U_{\mathfrak{m}} = \prod_{p \neq p_\infty} U_p^{(n_p)} \times \mathbb{R}_{>0}$. Let $m = m' p^{n_p}$. Then $U_p^{(n_p)}$ is certainly contained in the norm group of the unramified extension $\mathbb{Q}_p(\zeta_{m'})/\mathbb{Q}_p$ from **Homework 6.2(3)**, but also in the norm group of $\mathbb{Q}_p(\zeta_{p^{n_p}})/\mathbb{Q}_p$ according to **Lemma 7.1**.

This means that

$$U_{\mathfrak{m}} \subseteq \mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathbb{I}_{\mathbb{Q}(\zeta_m)}).$$

Thus:

$$\overline{U}_{\mathfrak{m}} \subseteq N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)}) \subseteq C_{\mathbb{Q}}$$

By the **Classification of Finite Abelian Extensions (Global Version)**, this implies that $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}_{\mathfrak{m}}$.

On the other hand,

$$1 = \frac{\varphi(\mathfrak{m}_0)}{\varphi(m)} = \frac{|\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})|} = \frac{|C_{\mathbb{Q}}/\overline{U}_{\mathfrak{m}}|}{|\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})|} = \frac{|\operatorname{Gal}(\mathbb{Q}_{\mathfrak{m}}/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})|}$$

by **Example 7.2** and **Proposition 7.2**. So we have $\mathbb{Q}_{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$. □

Proof of (a) (another easier version). We still want to prove:

$$\overline{U}_{\mathfrak{m}} \subseteq N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)}) = \ker(\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : C_{\mathbb{Q}} \to \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$$

It suffices to show:

$$U_{\mathfrak{m}} \subseteq \ker(\mathbb{I}_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$$

For all $x := (x_\infty, x_p)_p \in U_{\mathfrak{m}}$, denote the natural embedding $\iota_p : \mathbb{Q}_p^* \to \mathbb{I}_{\mathbb{Q}}$ and $\iota_\infty : \mathbb{R}^* \to \mathbb{I}_{\mathbb{Q}}$. Then:

$$x = \prod_{p \text{ prime}} \iota_p(x_p) \cdot \iota_\infty(x_\infty)$$

- **Claim:** For all prime number p, we have

$$\iota_p(x_p) \in \ker(\mathbb{I}_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$$

Recall **Corollary 5.1**: for prime number p, write $m = p^r \cdot n$ with $\gcd(p, n) = 1$. Then following map

$$f_p : \mathbb{Q}_p^* \xrightarrow{\iota_p} \mathbb{I}_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\simeq} (\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\simeq} (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

can be specifically described as:

$$a \in \mathbb{Z}_p^* \mapsto (\overline{a}^{-1}, \overline{1})$$
$$p \mapsto (\overline{1}, \overline{p})$$

so for $p \nmid n$, from the definition of $U_{\mathfrak{m}}$ we have $x_p \in \mathbb{Z}_p^*$, so $f_p(x_p) = \overline{1} \in (\mathbb{Z}/m\mathbb{Z})^*$; for $p \mid n$, also from the definition of $U_{\mathfrak{m}}$ we have $x_p \equiv 1 \pmod{p^r}$, so $f_p(x_p) = (\overline{1}, \overline{1}) \in (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Hence the claim is proved.

The map $\mathbb{R}^* \xrightarrow{\iota_\infty} \mathbb{I}_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is trivial, hence $x \in \ker(\mathbb{I}_{\mathbb{Q}} \xrightarrow{\text{quotient}} C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$. So $\overline{U}_{\mathfrak{m}} \subseteq \ker(C_{\mathbb{Q}} \xrightarrow{\psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$.

The proof of equivalence is the same as above. □

Solution of (b). Because ∞ is not in the modulus, i.e. ∞ is unramified in $\mathbb{Q}_{\mathfrak{m}}$, the ray class field $\mathbb{Q}_{\mathfrak{m}}$ must be contained in $\mathbb{R}$.

Also:

$$[\mathbb{Q}_{(m)\infty} : \mathbb{Q}_{(m)}] = [\overline{U}_{(m)} : \overline{U}_{(m)\infty}] \leqslant [U_{(m)} : U_{(m)\infty}] = 2$$

Hence by (a) $\mathbb{Q}_{\mathfrak{m}}$ is the maximal real subfield of $\mathbb{Q}(\zeta_m)$, i.e. $\mathbb{Q}_{\mathfrak{m}} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. And the "$\leqslant$" is actually "$=$". □

Solution of (c). The following lemma comes from Keqin Feng's *Algebraic Number Theory*.

Lemma 7.2. d is a square free integer. Then the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Q}(\zeta_{|D|})$, where $D = \mathrm{Disc}(\mathbb{Q}(\sqrt{d}))$.

From the Lemma we can immediately get the conductor of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$:

- If $d \in \mathbb{N}^*$, then the conductor is $(|D|)$.
- If $d < 0$, then the conductor is $(|D|)\infty$.

□

Solution of (d). $\mathbb{Q}[\sqrt{-5}], \mathbb{Q}[i] \subseteq \mathbb{Q}_{[}\zeta_{20}]$ and this is the smallest cyclotomic field containing $\mathbb{Q}[\sqrt{-5}, i]$. So the conductor of $\mathbb{Q}[\sqrt{-5}, i]/\mathbb{Q}$ is $(20)\infty$. □

Homework 7.3. Compute $\mathrm{Cl}(K)$ and $\mathrm{Cl}^+(K)$ for the fields $K = \mathbb{Q}[\sqrt{2}]$ and $K = \mathbb{Q}[\sqrt{3}]$ respectively.

Solution. (i) $K = \mathbb{Q}[\sqrt{2}]$:

By the Minkowski bound, easily we get $\mathrm{Cl}(K) = \{1\}$.

$\mathcal{I}_{K,(1)} = \mathcal{I}_{K,(1)\mathfrak{m}}$,

$$\mathbb{Q}[\sqrt{2}]^*_{(1)\mathfrak{m}} := \{q_1 + q_2\sqrt{2} : q_1 + q_2\sqrt{2}, q_1 - q_2\sqrt{2} > 0, q_1, q_2 \in \mathbb{Q}\}$$

Notice that for all $q_1 + q_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]^*$,

- If $q_1 + q_2\sqrt{2}, q_1 - q_2\sqrt{2} > 0$, then $(q_1 + q_2\sqrt{2}) = (q_1 + q_2\sqrt{2})$.
- If $q_1 + q_2\sqrt{2}, q_1 - q_2\sqrt{2} < 0$, then $(q_1 + q_2\sqrt{2}) = (-q_1 - q_2\sqrt{2})$.
- If $q_1 + q_2\sqrt{2} < 0, q_1 - q_2\sqrt{2} > 0$, then consider $q_1' + q_2'\sqrt{2} := (q_1 + q_2\sqrt{2})(1 - \sqrt{2})$. Then $(q_1' + q_2'\sqrt{2})(q_1' - q_2'\sqrt{2}) > 0$, which implies $q_1' + q_2'\sqrt{2}, q_1' - q_2'\sqrt{2} > 0$ or the opposite. Also we have $(q_1 + q_2\sqrt{2}) = (\pm q_1' \pm q_2'\sqrt{2})$.
- If $q_1 + q_2\sqrt{2} > 0, q_1 - q_2\sqrt{2} < 0$, similar to the above.

So we have:

$$\mathrm{Im}(\mathbb{Q}^* \to \mathcal{I}) = \mathrm{Im}(\mathbb{Q}[\sqrt{2}]^*_{(1)\mathfrak{m}} \to \mathcal{I})$$

Hence $\mathrm{Cl}^+(K) = \{1\}$.

(ii) $K = \mathbb{Q}[\sqrt{3}]$:

By the Minkowski bound, easily we get $\mathrm{Cl}(K) = \{1\}$.

We claim that:

$$\mathrm{Im}(\mathbb{Q}[\sqrt{3}]^*_{(1)\mathfrak{m}} \to \mathcal{I}) = \{(q_1 + q_2\sqrt{3}) : q_1^2 - 3q_2^2 \in \mathbb{Q}_{>0}\}$$
$$\mathcal{I} = \{(q_1 + q_2\sqrt{3}) : q_1^2 - 3q_2^2 \in \mathbb{Q}_{>0}\} \sqcup \{(q_1 + q_2\sqrt{3}) : q_1^2 - 3q_2^2 \in \mathbb{Q}_{<0}\}$$

Suppose $(q_1 + q_2\sqrt{3}) = (q_1' + q_2'\sqrt{3}) \in \mathcal{I}$ with $q_1^2 - 3q_2^2 > 0, q_1'^2 - 3q_2'^2 < 0$. Then there exists $u_1 + u_2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]^*$ such that:

$$(q_1 + q_2\sqrt{3})(u_1 + u_2\sqrt{3}) = q_1' + q_2'\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$

So $u_1, u_2 \in \mathbb{Z}$ and $u_1^2 - 3u_2^2 = -1$. It is impossible!

Hence the claim is true. So we have $\mathrm{Cl}^+(K) = \mathbb{Z}/2\mathbb{Z}$. □

8 2025.10.30

Definition 8.1. Let L/K be a finite abelian extension. We know that $L \subseteq K_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$. Let $N_{L/K}(\mathfrak{m})$ be the subgroup of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ generated by the classes of ideals $[\mathfrak{p}_v]^{f(v)}$ for all finite places $v \in V_{K,f}$ not dividing $\mathfrak{m}$, where the inertia degree is defined as $f(v) := f(w|v)$ for any place $w \in V_L$ lying over v.

Exercise 8.1. Show that the image of the composite map:

$$C_L \xrightarrow{N_{L/K}} C_K \longrightarrow C_K/\overline{U_{\mathfrak{m}}} \cong \mathrm{Cl}_{\mathfrak{m}}(K)$$

is the subgroup $N_{L/K}(\mathfrak{m})$.

8.1 Conclusion: Ideal-Theoretic Formulation of Global Class Field Theory

Theorem 8.1.

1. **(Existence)** For every modulus $\mathfrak{m}$, there exists a unique finite abelian extension $K_{\mathfrak{m}}/K$ such that a prime v is unramified in $K_{\mathfrak{m}}$ if and only if $v \nmid \mathfrak{m}$. The map from $\mathcal{I}_K^{\mathfrak{m}}$ to $\mathrm{Gal}(K_{\mathfrak{m}}/K)$, which sends a prime ideal $\mathfrak{p}_v$ to its Frobenius element Frob_v, factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ and induces an isomorphism:
$$\mathrm{Cl}_{\mathfrak{m}}(K) \xrightarrow{\sim} \mathrm{Gal}(K_{\mathfrak{m}}/K)$$

2. **(Abstract Kronecker-Weber)** The maximal abelian extension of K is the union of all ray class fields:
$$K^{ab} = \bigcup_{\mathfrak{m}} K_{\mathfrak{m}}$$

3. **(Reciprocity)** For any finite abelian extension L/K, there exists an admissible modulus $\mathfrak{m}$ (i.e., $L \subseteq K_{\mathfrak{m}}$). The Artin reciprocity map
$$\begin{aligned} \mathrm{Cl}_{\mathfrak{m}}(K) &\longrightarrow \mathrm{Gal}(L/K) \\ [\mathfrak{p}_v] &\longmapsto \mathrm{Frob}_v \end{aligned}$$
is surjective with kernel $N_{L/K}(\mathfrak{m})$.

Corollary 8.1. Let L/K be a finite abelian extension and let $\mathfrak{m} = \mathfrak{f}_{L/K}$ be its conductor. The set of prime ideals of K that split in L is given by

$$\begin{aligned}\mathrm{Spl}_{L/K} &= \{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \text{ splits in } L\} \\ &= \{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \nmid \mathfrak{m} \text{ and the image of } [\mathfrak{p}] \text{ in } \mathrm{Cl}_{\mathfrak{m}}(K) \text{ lies in } N_{L/K}(\mathfrak{m})\}\end{aligned}$$

III. Arithmetic Applications

8.2 Hilbert Class Field

Definition 8.2.

1. Let H/K be the ray class field corresponding to the trivial modulus $\mathfrak{m}_{\text{triv}} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0 = (1)$ and $\mathfrak{m}_\infty = \emptyset$. This extension H is called the **Hilbert class field** of K.
2. Let H^+/K be the ray class field corresponding to the modulus $\mathfrak{m}^+ = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0 = (1)$ and $\mathfrak{m}_\infty = \{\text{all real places of } K\}$. This extension H^+ is called the **narrow Hilbert class field** of K. The corresponding ray class group $\mathrm{Cl}^+(K) := \mathrm{Cl}_{\mathfrak{m}^+}(K)$ is called the **narrow class group**.

Remark:

1. The trivial modulus $\mathfrak{m}_{\text{triv}}$ divides every modulus $\mathfrak{m}$. This implies an inclusion of ray class fields $H \subseteq K_{\mathfrak{m}}$. In particular, taking $\mathfrak{m} = \mathfrak{m}^+$, we have $H \subseteq H^+$.
2. From the main theorem, we have isomorphisms:
$$\begin{aligned}\mathrm{Cl}(K) &\cong \mathrm{Gal}(H/K) \cong C_K/\overline{U}_{\mathfrak{m}_{\text{triv}}} \\ \mathrm{Cl}^+(K) &\cong \mathrm{Gal}(H^+/K) \cong C_K/\overline{U}_{\mathfrak{m}^+}\end{aligned}$$
3. The natural map $\mathrm{Cl}^+(K) \to \mathrm{Cl}(K)$ is surjective, giving a short exact sequence:
$$\frac{K^* \cap U_{\mathfrak{m}_{\text{triv}}}}{K^* \cap U_{\mathfrak{m}^+}} \to \frac{U_{\mathfrak{m}_{\text{triv}}}}{U_{\mathfrak{m}^+}} \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 1$$
Simultaneously:
$$\frac{K^* \cap U_{\mathfrak{m}_{\text{triv}}}}{K^* \cap U_{\mathfrak{m}^+}} = \frac{\mathcal{O}_K^*}{\mathcal{O}_K^{*,+}}$$

where $\mathcal{O}_K^{*,+}$ denotes the group of totally positive units, i.e.

$$\mathcal{O}_K^{*,+} = \{x \in \mathcal{O}_K^* \mid \tau(x) > 0 \text{ for all real embeddings } \tau\}$$

And:

$$\frac{U_{\mathfrak{m}_{\text{triv}}}}{U_{\mathfrak{m}^+}} \cong \prod_{v \text{ real places}} \{\pm 1\}$$

Proposition 8.1.

1. The Hilbert class field H of K is the unique maximal abelian extension of K which is unramified at all places.
2. The narrow Hilbert class field H^+ of K is the maximal abelian extension of K which is unramified at all finite places of K.

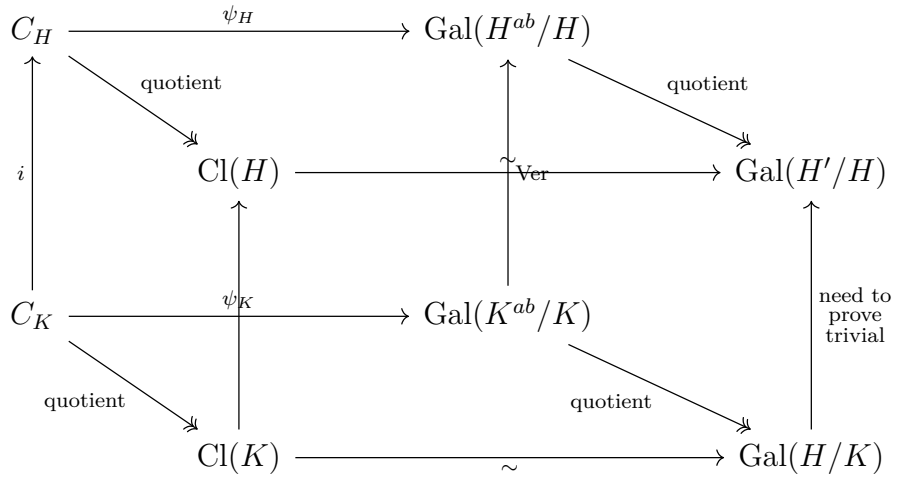
Proof. **Recall:** A place v is unramified in the ray class field $K_{\mathfrak{m}}/K$ if and only if $v \nmid \mathfrak{m}$. For any finite abelian extension L/K, a place v is ramified in L/K if and only if $v \mid \mathfrak{f}_{L/K}$.

Hence all places of K are unramified in H. Suppose L/K is a finite abelian extension such that all places of K are unramified in L. We want to show $L \subseteq H$. We have $L \subseteq K_{\mathfrak{m}}$ where $\mathfrak{m}$ is the conductor $\mathfrak{f}_{L/K}$. This implies that the modulus $\mathfrak{m}$ must be the trivial modulus, $\mathfrak{m} = \mathfrak{m}_{\text{triv}}$.

Similar argument works for (2). □

Theorem 8.2 (**Artin's Principal Ideal Theorem**)**.** The natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(H)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_H]$ is trivial. In particular, for every ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the ideal $\mathfrak{a}\mathcal{O}_H$ is principal.

Fact: For a finite group G, the Verlagerung map $\mathrm{Ver} : G^{ab} \to (G^{\mathrm{der}})^{ab}$ is a trivial homomorphism. (cf. Neukirch, Thm 7.6).



where H' is the Hilbert class field of H.

We should prove the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(H^{ab}/H) & \xrightarrow{\text{quotient}} & \mathrm{Gal}(H'/H) \\ \uparrow{\scriptstyle \mathrm{Ver}} & & \uparrow{\scriptstyle \text{need to prove trivial}} \\ \mathrm{Gal}(K^{ab}/K) & \xrightarrow[\text{quotient}]{} & \mathrm{Gal}(H/K) \end{array}$$

In one homework, we have proved that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(H^{ab}/H) = \mathrm{Gal}(\overline{H}/H)^{ab} & \xrightarrow{\text{quotient}} & \mathrm{Gal}(H'/H) \\ \uparrow{\scriptstyle \mathrm{Ver}} & & \uparrow{\scriptstyle \mathrm{Ver}} \\ \mathrm{Gal}(K^{ab}/K) = \mathrm{Gal}(\overline{K}/K)^{ab} & \longrightarrow & \mathrm{Gal}(H'/K)^{ab} \end{array}$$

Claim 1: $\mathrm{Gal}(H'/K)^{ab} = \mathrm{Gal}(H/K)$. This is because: H'^{ab} contains H because H' contains H. For every place of K, it is unramified in H/K, and for every place of H is unramified in H'/H, hence every place of K is unramified in H'^{ab}. Because H is the maximal abelian extension of K unramified at all places, H'^{ab} must be contained in H. Hence:

$$\mathrm{Gal}(H'/K)^{ab} = \mathrm{Gal}(H'^{ab}/K) = \mathrm{Gal}(H/K)$$

Claim 2: $\mathrm{Gal}(H'/H) = \mathrm{Gal}(H'/K)^{\mathrm{der}}$. From Claim 1,

$$\mathrm{Gal}(H'/H) \cong \mathrm{Gal}(H'/K)/\mathrm{Gal}(H'/H) \cong \mathrm{Gal}(H'/K)/\mathrm{Gal}(H'/K)^{ab} \cong \mathrm{Gal}(H'/K)^{\mathrm{der}}$$

Finally the theorem is got proved by the **Fact**. □

8.3 Hecke L-functions

Recall:

1. **Dedekind zeta function.** For a number field K.

$$\zeta_K(s) = \sum_{0\neq\mathfrak{a}\subseteq\mathcal{O}_K \text{ ideal}} \frac{1}{N(\mathfrak{a})^s} = \prod_{0\neq\mathfrak{p}\subseteq\mathcal{O}_K \text{ prime}} \frac{1}{1-N(\mathfrak{p})^{-s}}$$

   It has a meromorphic continuation to $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ with a simple pole at $s = 1$.

2. **Dirichlet L-function.** A Dirichlet character is a homomorphism $\chi_c : (\mathbb{Z}/c\mathbb{Z})^* \to S^1$.

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p\nmid c} \frac{1}{1-\chi(p)p^{-s}}$$

   If $\chi = 1$ (the trivial character), then $L(\chi, s) = \zeta(s)$. If $\chi \neq 1$, then $L(\chi, s)$ has a holomorphic continuation to $\mathrm{Re}(s) > 0$.

The Hecke L-function generalizes both of these L-functions.

Definition 8.3. 1. A **Hecke character** of K is a continuous homomorphism $\chi : C_K \to S^1$.

2. We define the **Hecke L-function** for a Hecke character χ.

$$L(\chi, s) = \prod_{v \text{ finite}} \frac{1}{1-\chi(v)(N(\mathfrak{p}_v))^{-s}}$$

   where for a finite place v corresponding to the prime ideal $\mathfrak{p}_v$,

$$\chi(v) = \begin{cases} \chi_v(\pi_v) & \text{if } \chi_v(\mathcal{O}_{K_v}^*) = \{1\} \text{ (i.e., } \chi \text{ is unramified at } v) \\ 0 & \text{otherwise (i.e., } \chi \text{ is ramified at } v) \end{cases}$$

   where π_v is any uniformizer of the local field K_v, and χ_v is defined by the following composition:

$$K_v^* \xrightarrow{\iota_v} \mathbb{I}_K \xrightarrow{\text{quotient}} C_K \xrightarrow{\chi} S^1$$

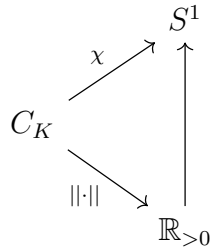
Example 8.1.

1. If $\chi = \chi_0 := 1$ (the trivial character), then $L(\chi_0, s) = \zeta_K(s)$.

2. If $K = \mathbb{Q}$ and $\chi : C_{\mathbb{Q}} \to S^1$ is a Hecke character, it corresponds to a character $\tilde{\chi}$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ for some minimal integer N. Then $L(\chi, s) = L(\tilde{\chi}, s)$ is the classical Dirichlet L-function.

Fact: A Hecke L-function has a meromorphic continuation to the region $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$. If the restriction of χ to the norm-1 idele class group, $\chi|_{C_K^1}$, is not the trivial character, then the L-function is holomorphic in this region.

If $\chi|_{C_K^1} = 1$, then χ can factor through $\mathbb{R}_{>0}$:



A continuous character from $\mathbb{R}_{>0}$ to S^1 must be of the form $\chi(x) = ||x||^{it}$ for some $t \in \mathbb{R}$. Then for an unramified finite place v, we have $\chi(v) = \chi_v(\pi_v) = ||\pi_v||^{it} = N(\mathfrak{p}_v)^{it}$. The L-function is then:

$$\begin{aligned} L(\chi, s) &= \prod_{v \text{ finite}} \frac{1}{1 - \chi(v)N(\mathfrak{p}_v)^{-s}} = \prod_{v \text{ finite}} \frac{1}{1 - N(\mathfrak{p}_v)^{-(s-it)}} \\ &= \zeta_K(s - it) \end{aligned}$$

(**Note:** So in this case the Hecke L-function has a pole at $s = 1 + it$.)

Fact: Indeed, Tate's Thesis shows that a Hecke L-function has a meromorphic continuation to the entire complex plane $\mathbb{C}$.

Definition 8.4. If a Hecke character $\chi : C_K \to S^1$ factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ for some modulus $\mathfrak{m}$, then the corresponding L-function $L(\chi, s)$ is called a **Weber L-function**.

Definition 8.5. The L-function associated to the character $\tilde{\chi} : \mathrm{Cl}_{\mathfrak{m}}(K) \to S^1$ is defined

as

$$\begin{aligned} L_{K,\mathfrak{m}}(s,\tilde{\chi}) &:= L(\chi,s) \\ &= \prod_{\substack{v\in V_{K,f}\\ v\nmid \mathfrak{m}_0}} \frac{1}{1-\chi(v)N(\mathfrak{p}_v)^{-s}} \\ &= \prod_{\substack{v\in V_{K,f}\\ v\nmid \mathfrak{m}_0}} \frac{1}{1-\tilde{\chi}(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-s}} = \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K\\ \text{coprime to } \mathfrak{m}_0}} \tilde{\chi}(\mathfrak{a})(N\mathfrak{a})^{-s} \end{aligned}$$

If $\tilde{\chi}\neq 1$, then $L_{K,\mathfrak{m}}(s,\tilde{\chi})$ is holomorphic on $\mathrm{Re}(s) > 1-\frac{1}{[K:\mathbb{Q}]}$.

Recall: If $K/\mathbb{Q}$ is a finite abelian extension, then by the Kronecker-Weber theorem, $K\subseteq\mathbb{Q}(\zeta_N)$ for some integer N. This gives a surjective homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^* \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

So there is a natural injection of character groups:

$$\widehat{\mathrm{Gal}(K/\mathbb{Q})} \hookrightarrow \widehat{(\mathbb{Z}/N\mathbb{Z})^*}$$

The Dedekind zeta function of K factors as a product of Dirichlet L-functions:

$$\zeta_K(s) = \prod_{\chi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}} L(\chi,s) = \zeta(s) \prod_{\substack{\chi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}\\ \chi\neq 1}} L(\chi,s)$$

This implies that $L(\chi,1)\neq 0,\infty$ for all non-trivial characters χ.

Generalizing this to any number field K_0: Let K/K_0 be a finite abelian extension. By global class field theory, $K\subseteq(K_0)_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$ with conductor $\mathfrak{f}_{K/K_0}$. We have a surjective map from the ray class group to the Galois group:

$$\mathrm{Gal}((K_0)_{\mathfrak{m}}/K_0) \cong \mathrm{Cl}_{\mathfrak{m}}(K_0) \twoheadrightarrow \mathrm{Gal}(K/K_0)$$

So there is a natural injection of character groups:

$$\widehat{\mathrm{Gal}(K/K_0)} \hookrightarrow \widehat{\mathrm{Cl}_{\mathfrak{m}}(K_0)}$$

This implies a factorization of the Dedekind zeta function:

$$\zeta_K(s) = \zeta_{K_0}(s) \prod_{\substack{\chi \in \widehat{\mathrm{Gal}(K/K_0)} \\ \chi \neq 1}} L_{K_0,\mathfrak{m}}(\chi, s)$$

In particular, this implies that $L_{K_0,\mathfrak{m}}(\chi, 1) \neq 0, \infty$ for all non-trivial characters χ.

8.4 Distribution of primes

Recall: The Dedekind zeta function $\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K \text{ prime}} \frac{1}{1-N(\mathfrak{p})^{-s}}$ has a simple pole at $s = 1$. This implies that as $s \to 1^+$,

$$\log \zeta_K(s) \sim \log \frac{1}{s-1} \sim \sum_{\mathfrak{p} \subseteq \mathcal{O}_K \text{ prime}} N(\mathfrak{p})^{-s}$$

Definition 8.6. For a set T of finite places of K, we define the **Dirichlet density** of T, denoted $\rho(T)$, as

$$\rho(T) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}}$$

if the limit exists.

Exercise 8.2. Let L/K be a finite extension. Let $T = \{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \mid f(\mathfrak{P}|\mathfrak{p}) = 1 \text{ with } \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}$. Then show that $\rho(T) = 1$.

Proposition 8.2. Let L/K be a finite Galois extension. Then the density of the set of primes that split completely is

$$\rho(\mathrm{Spl}_{L/K}) = \frac{1}{[L:K]}$$

Proof Sketch. From **Exercise 8.2**:

$$\sum_{\mathfrak{p} \in \mathrm{Spl}_{L/K}} N(\mathfrak{p})^{-s} = \frac{1}{[L:K]} \sum_{\substack{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \\ e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1}} (N\mathfrak{P})^{-s}$$
$$\sim \frac{1}{[L:K]} \sum_{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime}} (N\mathfrak{P})^{-s} \sim \frac{1}{[L:K]} \log \frac{1}{s-1}$$

□

Exercise 8.3.

1. Let L_1, L_2 be two finite extensions of K. Show that
$$\mathrm{Spl}_{L_1L_2/K} = \mathrm{Spl}_{L_1/K} \cap \mathrm{Spl}_{L_2/K}$$
2. Let L/K be a finite extension, and let L'/K be its Galois closure. Then $\mathrm{Spl}_{L/K} = \mathrm{Spl}_{L'/K}$.

In particular, $\rho(\mathrm{Spl}_{L/K}) = \frac{1}{[L:K]}$ if and only if L/K is a Galois extension.

Corollary 8.2. Let L_1, L_2 be two finite Galois extensions of K. The following are equivalent:

1. $L_1 \subseteq L_2$
2. $\mathrm{Spl}_{L_2/K} \subseteq \mathrm{Spl}_{L_1/K}$
3. There exists a set of finite places $T \subseteq V_{K,f}$ with $\rho(T) = 0$ such that $\mathrm{Spl}_{L_2/K} \setminus T \subseteq \mathrm{Spl}_{L_1/K}$.

Proof. The implications (1) $\implies$ (2) and (2) $\implies$ (3) are clear. We show (3) $\implies$ (1).

From **Exercise 8.3**, we know that $\mathrm{Spl}_{L_1L_2/K} = \mathrm{Spl}_{L_1/K} \cap \mathrm{Spl}_{L_2/K}$. The condition (3) implies that $\mathrm{Spl}_{L_2/K} \setminus T \subseteq \mathrm{Spl}_{L_1/K} \cap \mathrm{Spl}_{L_2/K} = \mathrm{Spl}_{L_1L_2/K}$.

Taking the density of both sides, and since $\rho(T) = 0$, we have

$$\rho(\mathrm{Spl}_{L_2/K} \setminus T) = \rho(\mathrm{Spl}_{L_2/K}) \leq \rho(\mathrm{Spl}_{L_1L_2/K})$$

Using the density formula for Galois extensions, this becomes

$$\frac{1}{[L_2 : K]} \leq \frac{1}{[L_1L_2 : K]}$$

which implies $[L_1L_2 : K] \leq [L_2 : K]$. Since L_2 is a subfield of L_1L_2, we must have $[L_1L_2 : L_2] = 1$, which means $L_1L_2 = L_2$. This implies that $L_1 \subseteq L_2$. □

Recall: Dirichlet's density theorem. Let $N \geq 1$ be an integer and $a \in \mathbb{Z}$ with

$\gcd(a, N) = 1$. Then the set of primes p with $p \equiv a \pmod{N}$ has Dirichlet density

$$\frac{1}{\phi(N)} = \frac{1}{|(\mathbb{Z}/N\mathbb{Z})^*|}$$

Sketch of proof: For every character $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}$, consider the L-function $L(\chi, s) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$. As $s \to 1^+$, we have

$$\log L(\chi, s) = \sum_p \frac{\chi(p)}{p^s} + O(1)$$

Using orthogonality of characters, we sum over all χ:

$$\begin{aligned}\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}} \overline{\chi(a)} \log L(\chi, s) &= \sum_p \frac{1}{p^s} \sum_\chi \overline{\chi(a)}\chi(p) + O(1) \cdot |(\mathbb{Z}/N\mathbb{Z})^*| \\ &= |(\mathbb{Z}/N\mathbb{Z})^*| \sum_{p \equiv a \pmod{N}} \frac{1}{p^s} + O(1)\end{aligned}$$

The left side is dominated by the term for the trivial character χ_0, which is $\log L(\chi_0, s) \sim \log \frac{1}{s-1}$. The other terms are bounded since $L(1, \chi) \neq 0, \infty$ for $\chi \neq 1$. This gives the result.

For a general number field K, the role of Dirichlet L-functions is played by Weber L-functions. The role of the integer N is played by a modulus $\mathfrak{m}$, and the group $(\mathbb{Z}/N\mathbb{Z})^*$ is replaced by the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$.

Theorem 8.3 (**Generalized Dirichlet's Density Theorem**)**.** Let $\mathfrak{m}$ be a modulus of a number field K. Fix a class $\alpha \in \mathrm{Cl}_\mathfrak{m}(K)$. Let T be the set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p}$ is coprime to $\mathfrak{m}_0$ and the class of $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$ is α. Then the Dirichlet density of this set is

$$\rho(T) = \frac{1}{|\mathrm{Cl}_\mathfrak{m}(K)|}$$

The proof is similar to the proof of Dirichlet's density theorem.

8.5 Chebotarev density theorem

Theorem 8.4. Let L/K be a finite Galois extension. Fix a conjugacy class $C \subseteq \mathrm{Gal}(L/K)$. Let T be the set of prime ideals $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in L and the Frobenius class $[\mathrm{Frob}(\mathfrak{P}|\mathfrak{p})]$ is equal to C for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. Then the Dirichlet density of this set is

$$\rho(T) = \frac{|C|}{[L:K]}$$

Remark: We have already proved the theorem for the special case where $L = K_{\mathfrak{m}}$ and $C = \{1\}$.

Proof Sketch. **Case 1: L/K is an abelian extension.** In this case, any conjugacy class C is a singleton, $C = \{\sigma\}$. We know $L \subseteq K_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$ (e.g., the conductor $\mathfrak{m} = \mathfrak{f}_{L/K}$). By class field theory, we have a surjective homomorphism

$$\mathrm{Gal}(K_{\mathfrak{m}}/K) \cong \mathrm{Cl}_{\mathfrak{m}}(K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

which maps the class of a prime ideal $[\mathfrak{p}]$ to its Frobenius element $\mathrm{Frob}_{\mathfrak{p}} := \mathrm{Frob}(\mathfrak{P}|\mathfrak{p})$. Let $\tilde{C} \subseteq \mathrm{Cl}_{\mathfrak{m}}(K)$ be the inverse image of C under this map. Then the set T is given by

$$T = \{\mathfrak{p} \subseteq \mathcal{O}_K \text{ prime} \mid \mathfrak{p} \nmid \mathfrak{m} \text{ and the image of } [\mathfrak{p}] \text{ lies in } \tilde{C}\}$$

By the Generalized Dirichlet Density Theorem, the density of this set is

$$\rho(T) = \frac{|\tilde{C}|}{|\mathrm{Cl}_{\mathfrak{m}}(K)|} = \frac{|C|}{|\mathrm{Gal}(L/K)|} = \frac{|C|}{[L:K]}$$

Case 2: L/K is not an abelian extension. (Idea: reduce to the abelian case). Fix an element $\sigma \in C$. Let $K' = L^{\langle\sigma\rangle}$ be the fixed field of the cyclic subgroup generated by σ. The extension L/K' is a cyclic (and thus abelian) extension.

$$\begin{array}{lll} L & \mathfrak{P} & T_L \\ \big| \text{abelian} & & \\ K' & \mathfrak{p}' & T_{K'} \\ \big| & & \\ K & \mathfrak{p} & T \end{array}$$

Let us define the set of primes in K' that correspond to σ:

$$T_{K'} := \{\mathfrak{p}' \subseteq \mathcal{O}_{K'} \mid \mathfrak{p}' \cap \mathcal{O}_K \text{ is unramified in } L, \mathrm{Frob}(\mathfrak{P}|\mathfrak{p}') = \sigma, \text{ and } f(\mathfrak{p}'|(\mathfrak{p}' \cap \mathcal{O}_K)) = 1\}$$

Note that for a prime $\mathfrak{p}$ of K, if $\mathfrak{p}'$ lies over it, we have $\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) = \mathrm{Frob}(\mathfrak{P}|\mathfrak{p}')^{f(\mathfrak{p}'|\mathfrak{p})}$. So for $\mathfrak{p}' \in T_{K'}$, we have $\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) = \sigma^1 = \sigma$.

Consider the natural restriction map:

$$\begin{aligned} T_{K'} &\to T \\ \mathfrak{p}' &\mapsto \mathfrak{p}' \cap \mathcal{O}_K \end{aligned}$$

Claim 1. The map $T_{K'} \to T$ is surjective, and each fibre has $\frac{[K':K]}{|C|}$ elements.

Claim 1 implies the theorem: Assuming Claim 1, we can relate the sums over the two sets. Since for each $\mathfrak{p} \in T$, there are $\frac{[K':K]}{|C|}$ primes $\mathfrak{p}' \in T_{K'}$ lying over it with $f(\mathfrak{p}'|\mathfrak{p}) = 1$ (so $N(\mathfrak{p}') = N(\mathfrak{p})$), we have:

$$\sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s} = \frac{|C|}{[K' : K]} \sum_{\mathfrak{p}' \in T_{K'}} N(\mathfrak{p}')^{-s}$$

The sum over $\mathfrak{p}' \in T_{K'}$ is for the abelian extension L/K', so by the abelian case of the theorem (Case 1), its density is $\frac{1}{[L:K']}$. Therefore, the density of T is:

$$\rho(T) = \frac{|C|}{[K' : K]} \cdot \rho(T_{K'}) = \frac{|C|}{[K' : K]} \cdot \frac{1}{[L : K']} = \frac{|C|}{[L : K]}$$

This proves the theorem.

To prove Claim 1, we introduce another set of primes, this time in the top field L.

$$T_L := \{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \mid \mathfrak{P} \text{ is unramified over } K, \text{ and } \mathrm{Frob}(\mathfrak{P}|(\mathfrak{P} \cap \mathcal{O}_K)) = \sigma\}$$

Claim 2.

1. The restriction map from ideals in L to ideals in K' maps the set T_L to $T_{K'}$ and it is bijective.
2. This map $T_L \to T$ is surjective, and each fibre has $\frac{[K':K]}{|C|}$ elements.

Claim 2 $\implies$ **Claim 1** is obvious.

Proof of Claim 2:

1. For $\mathfrak{P} \in T_L$, $\mathfrak{p}' := \mathfrak{P} \cap \mathcal{O}_{K'}$, $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$. To prove that $\mathfrak{p}' \in T_{K'}$, we want to show that $f(\mathfrak{p}'|\mathfrak{p}) = 1$.

   $\sigma = \mathrm{Frob}(\mathfrak{P}|\mathfrak{p})$. The Galois group of the residue field extension is generated by this Frobenius element: $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) = \langle\sigma\rangle$. The fixed field of this action is $k_{\mathfrak{p}}$, so $k_{\mathfrak{P}}^{\langle\sigma\rangle} = k_{\mathfrak{p}}$.

   Since $K' = L^{\langle\sigma\rangle}$, the automorphism σ fixes K' and thus stabilizes the prime ideal $\mathfrak{p}' \subseteq \mathcal{O}_{K'}$. This means σ acts on the residue field $k_{\mathfrak{p}'}$. The condition that σ fixes K' implies its action on $k_{\mathfrak{p}'}$ is trivial. Therefore, $k_{\mathfrak{p}'} \subseteq k_{\mathfrak{P}}^{\langle\sigma\rangle} = k_{\mathfrak{p}}$, which implies $f(\mathfrak{p}'|\mathfrak{p}) = [k_{\mathfrak{p}'} : k_{\mathfrak{p}}] = 1$.

   We now show that the map $T_L \to T_{K'}$ is bijective. It suffices to show for any $\mathfrak{p}' \in T_{K'}$ there exists a unique $\mathfrak{P} \in T_L$ such that $\mathfrak{P} \cap \mathcal{O}_{K'} = \mathfrak{p}'$.

   Since $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{O}_K$ is unramified in L, we have $e(\mathfrak{P}|\mathfrak{p}') = 1$. The inertia degree is $f(\mathfrak{P}|\mathfrak{p}') = |\langle\sigma\rangle| = [L : K']$. From the fundamental identity $efg = [L : K']$, we have $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}'$.

2. For any $\mathfrak{p} \in T$, we have $e(L|\mathfrak{p}) = 1$ and the inertia degree of any prime above it is $f(L|\mathfrak{p}) = |\langle\sigma\rangle| = [L : K']$. The number of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$ is given by the formula $g = \frac{[L:K]}{ef} = \frac{[L:K]}{1\cdot[L':K]} = [K' : K]$. For any $\tau \in \mathrm{Gal}(L/K)$, the Frobenius elements are related by conjugation: $\mathrm{Frob}(\tau\mathfrak{P}|\mathfrak{p}) = \tau\,\mathrm{Frob}(\mathfrak{P}|\mathfrak{p})\tau^{-1}$. Hence, the number of primes of L in the set T_L (i.e., those with Frobenius equal to σ) lying above a given $\mathfrak{p} \in T$ is $\frac{[K':K]}{|C|}$. □

□

8.6 Homework

Homework 8.1. Show that the image of the composite map:

$$\varphi : C_L \xrightarrow{N_{L/K}} C_K \xrightarrow{\pi} C_K/\overline{U_{\mathfrak{m}}} \cong \mathrm{Cl}_{\mathfrak{m}}(K)$$

is the subgroup $N_{L/K}(\mathfrak{m})$.

Proof.

Claim: $N_{L/K}(\mathfrak{m}) \subseteq \mathrm{Im}(\varphi)$.

For any prime ideal $\mathfrak{p}_v \subseteq \mathcal{O}_K$ such that $\mathfrak{p}_v \nmid \mathfrak{m}_0$, we have v is unramified in $K_{\mathfrak{m}}$, so is unramified in L. Choose $w \mid v$, π_w is an uniformizer of L_w, we will show that:

$$\begin{aligned} L_w &\xrightarrow{\iota} C_L \xrightarrow{\varphi} \mathrm{Cl}_{\mathfrak{m}}(K) \\ \pi_w &\mapsto \iota(\pi_w) \mapsto [\mathfrak{p}_v]^{f(v)} \end{aligned}$$

We have commutative diagram:

$$\begin{array}{ccccc} L_w & \xrightarrow{\iota_w} & \mathbb{I}_L & \xrightarrow{\text{quotient}} & C_L \\ \downarrow{\scriptstyle N_{L_w/K_v}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} \\ K_v & \xrightarrow{\iota_v} & \mathbb{I}_K & \xrightarrow{\text{quotient}} & C_K \end{array}$$

and we know that for $v \in V_{K,f}$ unramified in $K_{\mathfrak{m}}$,

$$K_v \to C_K \to C_K/\overline{U}_{\mathfrak{m}} \to \mathrm{Gal}(K_{\mathfrak{m}}/K) \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}(K)$$

maps π_v to $[\mathfrak{p}_v]$. And we know:

$$N_{L_w/K_v}(\pi_w \mathcal{O}_{L_w}^*) = \pi_w^{[L_w:K_v]} \mathcal{O}_{K_v}^* = \pi_v^{f(v)} \mathcal{O}_{K_v}^*$$

So the **Claim** is proved.

Claim: $N_{L/K}(\mathfrak{m}) \supseteq \mathrm{Im}(\varphi)$.

Consider:

$$S := \{w \in V_L : w \mid v,\ v \in V_K,\ v \mid \mathfrak{m}\}$$

It is a finite set.

We have known that:

$$\mathbb{I}_L^S \hookrightarrow C_L \text{ is dense.}$$

Because φ is continuous and $\mathrm{Cl}_{\mathfrak{m}}(K)$ is finite, for any $\overline{c} \in C_L$, we can choose $x \in \mathbb{I}_L^S$ such that:

$$\varphi(\overline{c}) = \varphi(\overline{x})$$

There is a finite set $T \subseteq V_K \setminus \{v \in V_K : v \mid \mathfrak{m}\}$ such that:

$$\begin{aligned}
\varphi(\overline{x}) &= \varphi\left(\overline{\prod_{v\in T}\prod_{w|v}\iota_w(x_w)\cdot\prod_{v\notin T}\prod_{w|v}\iota_w(x_w)}\right)\\
&= \pi\circ \mathrm{N}_{L/K}\left(\overline{\prod_{v\in T}\prod_{w|v}\iota_w(x_w)\cdot\prod_{v\notin T}\prod_{w|v}\iota_w(x_w)}\right)\\
&= \pi\left(\prod_{v\in T}\prod_{w|v}\mathrm{N}_{L/K}(\overline{\iota_w(x_w)})\cdot\prod_{v\notin T}\prod_{w|v}\mathrm{N}_{L/K}(\overline{\iota_w(x_w)})\right)\\
&= \pi\left(\prod_{v\in T}\prod_{w|v}\overline{\iota_v(\mathrm{N}_{L_w/K_v}(x_w))}\cdot\prod_{v\notin T}\prod_{w|v}\overline{\iota_v(\mathrm{N}_{L_w/K_v}(x_w))}\right)\\
&= \prod_{v\in T\setminus V_{K,\infty}}[\mathfrak{p}_v]^{\sum_{w|v}\mathrm{ord}_v(\mathrm{N}_{L_w/K_v}(x_w))}
\end{aligned}$$

where for all $v \notin T$, $w \mid v$, we have $x_w \in \mathcal{O}_{L_w}^*$, hence $\mathrm{N}_{L_w/K_v}(x_w) \in \mathcal{O}_{K_v}^*$. For all $v \in T \cap V_{K,\infty}$, $\pi \circ \iota_w$ is trivial because of $U_{\mathfrak{m}}$.

For any $v \in T \setminus V_{K,\infty}$, $w \mid v$:

$$\mathrm{ord}_v(\mathrm{N}_{L_w/K_v}(x_w)) = \mathrm{ord}_v(x_w^{[L_w:K_v]}) = \frac{\mathrm{ord}_w(x_w)[L_w:K_v]}{e(w|v)} \equiv 0 \pmod{f(w|v)}$$

So $\varphi(\overline{c}) = \varphi(\overline{x}) \in \mathrm{N}_{L/K}(\mathfrak{m})$. □

Remark: With the same method, we can also show that:

$$\langle [\mathfrak{p}_v] : v \nmid \mathfrak{m}_0\rangle = \mathrm{Cl}_{\mathfrak{m}}(K)$$

Homework 8.2. Let $K = \mathbb{Q}(\sqrt{-5})$.

(a) Compute the Hilbert class field H of K;

(b) Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. Show that $\mathfrak{p}$ is split in H if and only if $\mathfrak{p}$ is principal;

(c) (Lagrange) Let p denote odd prime numbers. Show that

$$\{p \equiv 1, 9 \pmod{20}\} = \{p \neq 5 \mid p = x^2 + 5y^2, x, y \in \mathbb{Z}\}.$$

Hint: Show that both sides equal to $\mathrm{Spl}_{H/\mathbb{Q}}$ which is the set of primes in $\mathbb{Q}$ that are split in H.

Solution of (a). We **Claim** $H = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

Denote $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1}) = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$. For any prime number p,

(i) If $p \neq 2, 5$, then p is both unramified in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{5})$, hence unramified in L.

(ii) If $p = 5$, then 5 is ramified in $\mathbb{Q}(\sqrt{5})$ with $e = 2, f = 1, g = 1$, while 5 is unramified in $\mathbb{Q}(\sqrt{-1})$ with $e = 1, f = 1, g = 2$, hence 5 is ramified in L with $e = 2, f = 1, g = 2$.

(iii) If $p = 2$, then 2 is unramified in $\mathbb{Q}(\sqrt{5})$ with $e = 1, f = 2, g = 1$, while 2 is ramified in $\mathbb{Q}(\sqrt{-1})$ with $e = 2, f = 1, g = 1$, hence 2 is ramified in L with $e = 2, f = 2, g = 1$.

For any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, denote $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$,

(i) If $p \neq 2, 5$, then p is unramified in K, hence $\mathfrak{p}$ is unramified in K.

(ii) If $p = 2, 5$, $e(\mathfrak{p}|p) = 2$. Because $2, 5$ is ramified in L with $e = 2$, so $\mathfrak{p}$ is unramified in L.

Hence L/K is unramified extension.

Because $[L : K] = 2$, $|\operatorname{Gal}(H/K)| = |\operatorname{Cl}(K)| = 2$, we have $H = L$. □

Proof of (b). We have isomorphism:

$$\operatorname{Cl}(K) \xrightarrow{\sim} \operatorname{Gal}(H/K)$$

mapping $[\mathfrak{p}]$ to $\mathrm{Frob}_{\mathfrak{p}}$.

Hence $\mathfrak{p}$ is split in H if and only if $\mathrm{Frob}_{\mathfrak{p}} = 1$ if and only if $[\mathfrak{p}] = 1$ if and only if $\mathfrak{p}$ is principal. □

Proof of (c). "$\supseteq$": If $p = x^2 + 5y^2$ and $p \neq 5$, then $p \equiv 1 \pmod 4), 1, 4 \pmod 5$, hence $p \equiv 1, 9 \pmod{20}$.

"$\subseteq$": If $p \equiv 1, 9 \pmod{20}$:

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{(p-1)\cdot(5-1)}{2}}\left(\frac{p}{5}\right) = 1$$

So p is unramified in K with $e = 1, f = 1, g = 2$.

Also because $p \equiv 1 \pmod 4$, p is split in $\mathbb{Q}(\sqrt{-1})$ with $e = 1, f = 1, g = 2$. Hence p is split in H with $e = 1, f = 1, g = 4$.

Choose any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over p, then $\mathfrak{p}$ is split in H, hence $\mathfrak{p}$ is principal by (b), say $\mathfrak{p} = (a + b\sqrt{-5})$. So:

$$p = N_{K/\mathbb{Q}}(\mathfrak{p}) = N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$$

□

Homework 8.3. Let L/K be a finite extension. Let $T = \{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \mid f(\mathfrak{P}|\mathfrak{p}) = 1 \text{ with } \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}$. Then show that $\rho(T) = 1$.

Proof. Consider $\log \zeta_L(s)$: On one hand when $s \to 1^+$:

$$\log \zeta_L(s) \sim \log \frac{1}{s-1}$$

On the other hand when $s \to 1^+$:

$$\begin{aligned}\log \zeta_L(s) &= \sum_{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime}} N(\mathfrak{P})^{-s} \\ &\sim \sum_{\substack{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \\ f(\mathfrak{P}|\mathfrak{p})=1}} N(\mathfrak{P})^{-s} + \sum_{\substack{\mathfrak{P} \subseteq \mathcal{O}_L \text{ prime} \\ f(\mathfrak{P}|\mathfrak{p}) \geqslant 2 \\ \mathfrak{p} \text{ unramified in } \mathcal{O}_L}} N(\mathfrak{P})^{-s}\end{aligned}$$

The second term can be bounded by:

$$0 \leqslant \sum_{\substack{\mathfrak{P}\subseteq\mathcal{O}_L \text{ prime} \\ f(\mathfrak{P}|\mathfrak{p})\geqslant 2 \\ \mathfrak{p} \text{ unramified in } \mathcal{O}_L}} N(\mathfrak{P})^{-s} \leqslant \sum_{p \text{ prime number}} [L:\mathbb{Q}] \cdot p^{-2s} < \infty$$

Hence when $s \to 1^+$:

$$\log \frac{1}{s-1} \sim \log \zeta_L(s) \sim \sum_{\mathfrak{P}\in T} N(\mathfrak{P})^{-s}$$

i.e. $\rho(T) = 1$. □

Homework 8.4.

(a) Let L_1 and L_2 be two finite extensions of K. Show that

$$\mathrm{Spl}_{L_1L_2/K} = \mathrm{Spl}_{L_1/K} \cap \mathrm{Spl}_{L_2/K}\,.$$

(b) Let L/K be a finite extension. Let L'/K be its Galois closure. Then $\mathrm{Spl}_{L/K} = \mathrm{Spl}_{L'/K}$. In particular, $\rho(\mathrm{Spl}_{L/K}) = \frac{1}{[L:K]}$ if and only if L/K is Galois.

Proof of (a). "$\subseteq$" : If $\mathfrak{p}$ is split in L_1L_2, then obviously $\mathfrak{p}$ is split in both L_1 and L_2.

"$\supseteq$" :

Let E be the Galois closure of L_1L_2 over K. For any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_E$ lying over $\mathfrak{p} \subseteq \mathcal{O}_K$, if the medium field M of E/K is M satisfies:

$$e(\mathfrak{P}_M|\mathfrak{p}) = f(\mathfrak{P}_M|\mathfrak{p}) = 1$$

where $\mathfrak{P}_M := \mathfrak{P} \cap \mathcal{O}_M$, note that:

$$D(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}(E/M) = D(\mathfrak{P}|\mathfrak{P}_M)$$

And we have:

$$|D(\mathfrak{P}|\mathfrak{P}_M)| = e(\mathfrak{P}|\mathfrak{P}_M)f(\mathfrak{P}|\mathfrak{P}_M) = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}) = |D(\mathfrak{P}|\mathfrak{p})| \geqslant |D(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}(E/M)|$$

So the equality holds, i.e.:

$$D(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(E/M)$$

If $\mathfrak{p}$ is split in both L_1 and L_2, for any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_E$ lying over $\mathfrak{p}$, we have:

$$e(\mathfrak{P}_{L_1}|\mathfrak{p}) = f(\mathfrak{P}_{L_1}|\mathfrak{p}) = 1, \quad e(\mathfrak{P}_{L_2}|\mathfrak{p}) = f(\mathfrak{P}_{L_2}|\mathfrak{p}) = 1$$

where $\mathfrak{P}_{L_i} = \mathfrak{P} \cap \mathcal{O}_{L_i}$. Hence:

$$D(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(E/L_1) \cap \mathrm{Gal}(E/L_2) = \mathrm{Gal}(E/L_1L_2)$$

So:

$$D(\mathfrak{P}|\mathfrak{P} \cap \mathcal{O}_{L_1L_2}) = D(\mathfrak{P}|\mathfrak{p})$$

In conclusion, for any prime ideal $\mathfrak{P} \subseteq \mathcal{O}_E$ lying over $\mathfrak{p}$,

$$e(\mathfrak{P}_{L_1L_2}|\mathfrak{p}) = f(\mathfrak{P}_{L_1L_2}|\mathfrak{p}) = 1$$

where $\mathfrak{P}_{L_1L_2} = \mathfrak{P} \cap \mathcal{O}_{L_1L_2}$. So $\mathfrak{p}$ is split in L_1L_2. □

Proof of (b). $\mathrm{Spl}_{L'/K} \subseteq \mathrm{Spl}_{L/K}$ is trivial. For any $\mathfrak{p} \in \mathrm{Spl}_{L/K}$ and $\sigma \in \mathrm{Gal}(L'/K)$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \dots \mathfrak{P}_g$$

with $e(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}_i|\mathfrak{p}) = 1$ for all $1 \leqslant i \leqslant g$. Then:

$$\mathfrak{p}\mathcal{O}_{\sigma(L)} = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{P}_1) \dots \sigma(\mathfrak{P}_g)$$

with $\sigma(\mathfrak{P}_i)$ being prime ideal of $\mathcal{O}_{\sigma(L)}$ lying over $\mathfrak{p}$, and $e(\sigma(\mathfrak{P}_i)|\mathfrak{p}) = f(\sigma(\mathfrak{P}_i)|\mathfrak{p}) = 1$ for all $1 \leqslant i \leqslant g$. Hence $\mathfrak{p}$ is split in $\sigma(L)$ for all $\sigma \in \mathrm{Gal}(L'/K)$.

So from (a):

$$\mathrm{Spl}_{L/K} = \bigcap_{\sigma \in \mathrm{Gal}(L'/K)} \mathrm{Spl}_{\sigma(L)/K} = \mathrm{Spl}_{L'/K}$$

By **Proposition 8.2**:

$$\rho(\mathrm{Spl}_{L/K}) = \rho(\mathrm{Spl}_{L'/K}) = \frac{1}{[L' : K]} = \frac{1}{[L : K]} \iff L = L' \text{ (i.e. } L/K \text{ is Galois)}$$

□

9 2025.11.06

9.1 Artin L-functions

Recall: The Artin reciprocity law gives a map $\psi_K : C_K \to \mathrm{Gal}(\overline{K}/K)^{ab}$. This relates to Hecke L-functions via characters:

$$\begin{aligned} \chi : C_K \to S^1 \quad &\text{(Hecke character)} \\ \rightsquigarrow L(\chi, s) \quad &\text{(Hecke L-function)} \end{aligned}$$

Goal: Given a continuous character (a 1-dimensional representation)

$$\rho : \mathrm{Gal}(\overline{K}/K) \to S^1$$

we want to define its L-function, $L(\rho, s)$. This is the so-called **Artin L-function**.

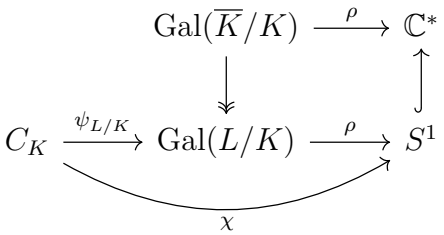
More generally, we can consider a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V)$$

where V is a finite-dimensional complex vector space.

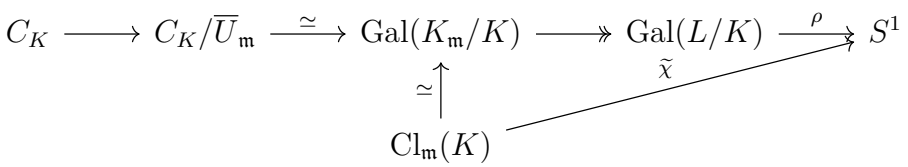
Exercise 9.1. The representation ρ always factors through the Galois group of a finite Galois extension, $\mathrm{Gal}(L/K)$, for some field L. (The essential reason for this is that the topology on $\mathbb{C}$ is very different from the profinite topology of the Galois group).

Using **Exercise 9.1**: when the dimension of V is 1, we have:



We hope to have $L(\rho, s) = L(\chi, s)$.

We know that $L \subseteq K_{\mathfrak{m}}$ where $\mathfrak{m} = \mathfrak{f}_{L/K}$ is the conductor of the extension L/K.



Let $\tilde{\chi}$ be the corresponding character on the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$.

Then we define the L-function as:

$$\begin{aligned} L(\rho, s) &= L(\chi, s) \\ &= L_{K,\mathfrak{m}}(\tilde{\chi}, s) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \frac{1}{1 - \tilde{\chi}([\mathfrak{p}])N(\mathfrak{p})^{-s}} \\ &= \prod_{\mathfrak{p} \text{ unramified in } L} \frac{1}{1 - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s}} \end{aligned}$$

For a general representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C})$. Suppose the kernel of the representation is $\ker \rho = \mathrm{Gal}(\overline{K}/L)$. It is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$, so by **Exercise 9.1**, L is a finite Galois extension of K, and ρ factors through $\mathrm{Gal}(L/K)$.

Definition 9.1. Define the **Artin L-function** for ρ as the product over unramified primes:

$$L(\rho, s) = L_K(\rho, s) := \prod_{\substack{\mathfrak{p} \in V_{K,f} \\ \text{unramified in } L}} \frac{1}{\det(I - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s})}$$

Artin's Conjecture: If ρ is an irreducible representation, then $L(\rho, s)$ extends to a holomorphic function on $\mathbb{C}$.

Remark: Class Field Theory implies that for a 1-dimensional representation ($\dim \rho = 1$), the Artin L-function $L(\rho, s)$ is equal to a Hecke L-function $L(\chi, s)$. In this case, Artin's conjecture holds.

Theorem 9.1. As an application of Class Field Theory, we can show that any Artin L-function $L(\rho, s)$ has a meromorphic continuation to $\mathbb{C}$.

Idea: Reduce the problem to the 1-dimensional case. We will prove this theorem later.

Question: How do we define the local factor corresponding to $\rho(\mathrm{Frob}_{\mathfrak{p}})$ when the prime $\mathfrak{p}$ is ramified in L?

Definition 9.2 (Complete Artin L-function $\widehat{L}(\rho, s)$). For any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, choose a prime ideal $\mathfrak{P} \subseteq \mathcal{O}_L$ lying above $\mathfrak{p}$. We have the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ and its normal subgroup, the inertia group $I(\mathfrak{P}|\mathfrak{p})$. The quotient group is isomorphic

to the Galois group of the residue fields:

$$D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$$

Choose any element $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} \in D(\mathfrak{P}|\mathfrak{p})$ that is a lifting of the Frobenius automorphism of the residue fields. Consider the characteristic polynomial

$$\det(I - \rho(\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}})N(\mathfrak{p})^{-s}|_{V^{I(\mathfrak{P}|\mathfrak{p})}})$$

(little exercise: $D(\mathfrak{P}|\mathfrak{p})$ acts on the subspace $V^{I(\mathfrak{P}|\mathfrak{p})}$, using the property of normal subgroup.)
This expression does not depend on the choice of the prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$, nor on the choice of the lifting $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}$. When $\mathfrak{p}$ is unramified in L, the inertia group is trivial, so $V^{I(\mathfrak{P}|\mathfrak{p})} = V$, and this expression simplifies to $\det(I - \rho(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s})$.
The **completed Artin L-function** is then defined as

$$\widehat{L}(\rho, s) = \prod_{\mathfrak{p} \in V_{K,f}} \frac{1}{\det(I - \rho(\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}})N(\mathfrak{p})^{-s}|_{V^{I(\mathfrak{P}|\mathfrak{p})}})}$$

Remark: The completed L-function $\widehat{L}(\rho, s)$ differs from the original definition $L(\rho, s)$ by only a finite number of Euler factors (the ramified primes). These factors are holomorphic and non-zero. Hence, Artin's conjecture for $L(\rho, s)$ and for $\widehat{L}(\rho, s)$ are equivalent.

Back to the idea of the proof of the theorem.

Sketch of the proof. First we list some **facts**:

1. **(Brauer's Theorem)**: Let G be a finite group and let ρ be a finite-dimensional complex representation of G. Then there exist subgroups $H_1, \ldots, H_r$ of G, one-dimensional representations ρ_i of H_i for each $1 \leq i \leq r$, and integers $n_1, \ldots, n_r \in \mathbb{Z}$ such that

   $$\rho = \sum_{i=1}^{r} n_i \, \mathrm{Ind}_{H_i}^{G} \rho_i$$

   (as virtual representations).

2. $\widehat{L}(\rho_1 \oplus \rho_2, s) = \widehat{L}(\rho_1, s) \cdot \widehat{L}(\rho_2, s)$.

3. Let E/K be a finite extension and let $\rho : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}(V)$ be a representation. Then

   $$\widehat{L}_K(\mathrm{Ind}_{\mathrm{Gal}(\overline{E}/E)}^{\mathrm{Gal}(\overline{K}/K)} \rho, s) = \widehat{L}_E(\rho, s).$$

By Brauer's theorem, we can write the representation ρ as a virtual sum of induced 1-dimensional representations for some finite Galois extension E/K:

$$\rho = \sum_{i=1}^{r} n_i \operatorname{Ind}_{\mathrm{Gal}(\overline{K}/E_i)}^{\mathrm{Gal}(\overline{K}/K)} \rho_i$$

where each E_i/K finite extension and $\rho_i : \mathrm{Gal}(\overline{E_i}/E_i) \to \mathbb{C}^*$ is a 1-dimensional character. Using the properties of the L-function:

$$\widehat{L}_K(\rho, s) = \prod_{i=1}^{r} \widehat{L}_K(\operatorname{Ind}_{\mathrm{Gal}(\overline{E_i}/E_i)}^{\mathrm{Gal}(\overline{K}/K)} \rho_i, s)^{n_i} = \prod_{i=1}^{r} \widehat{L}_{E_i}(\rho_i, s)^{n_i}$$

Each $\widehat{L}_{E_i}(\rho_i, s)$ is the L-function of a 1-dimensional character, which has a meromorphic continuation to $\mathbb{C}$. Since $\widehat{L}_K(\rho, s)$ is a product of powers of meromorphic functions, it is also meromorphic. □

Langlands Program

Class Field Theory establishes a fundamental correspondence:

$$\left\{\begin{array}{c}\text{1-dimensional continuous}\\ \text{representations of } \mathrm{Gal}(\overline{K}/K)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{certain 1-dimensional representations}\\ \text{of } \mathbb{A}_K^* \text{ (Hecke characters)}\end{array}\right\}$$

Langlands Conjecture: There exists a correspondence between

$$\left\{\begin{array}{c}\text{certain } n\text{-dimensional representations}\\ \text{of } \mathrm{Gal}(\overline{K}/K)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{certain automorphic}\\ \text{representations of } \mathrm{GL}_n(\mathbb{A}_K)\end{array}\right\}$$

This correspondence links the associated L-functions:

$$\text{Artin L-function} \longleftrightarrow \text{Automorphic L-function}$$

Artin L-functions arises from automorphic L-functions.

IV. Group Cohomology and Homology

9.2 G-modules

Let G be a group.

Definition 9.3. 1. A **(left) G-module** is an abelian group A with a left action of G, i.e., there is a group homomorphism $G \to \mathrm{Aut}(A)$.

2. $\mathrm{Hom}_G(A, A')$ is the set of G-module homomorphisms.

3. Mod_G is the category of G-modules, which is an abelian category.

Remark: The group ring $\mathbb{Z}[G]$ is the group algebra of G. The ring is not commutative if G is not an abelian group. A G-module is equivalent to a $\mathbb{Z}[G]$-module.

Example 9.1. 1. Let A be an abelian group and G be any group. We can define the **trivial action** of G on A by $g \cdot a = a$ for all $g \in G$ and $a \in A$.

2. Let $A = \mathbb{Z}[G]$. Then G acts on A by left multiplication.

3. Let L/K be a Galois finite extension. Let $A = L^*$ (the multiplicative group of the field) and $G = \mathrm{Gal}(L/K)$. The Galois action makes L^* a G-module.

4. If $G = \{e\}$ is the trivial group, then a G-module is just an abelian group.

Fact: For any G-module A in the category Mod_G, the functors $\mathrm{Hom}_G(-, A)$ and $\mathrm{Hom}_G(A, -)$ are both left exact.

Definition 9.4.

1. We say a G-module A is **projective** if the functor $\mathrm{Hom}_G(A, -)$ is exact.

2. We say a G-module A is **injective** if the functor $\mathrm{Hom}_G(-, A)$ is exact.

Example 9.2.

1. A G-module is projective if and only if it is a direct factor of a free $\mathbb{Z}[G]$-module.

2. If $G = \{e\}$ is the trivial group, every divisible abelian group is an injective G-module (e.g., $\mathbb{Q}$).

3. The direct sum of projective modules is projective. The direct product of injective modules is injective.

Definition 9.5. Let H be a subgroup of G.

1. **Co-induction:** The co-induction functor $\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ is defined by

$$A \mapsto \mathrm{Ind}_H^G(A) := \mathrm{Hom}_H(\mathbb{Z}[G], A) = \{f : G \to A \mid f(hg) = hf(g)\}$$

   where the structure of the (**left**) G-module on $\mathrm{Ind}_H^G(A)$ is given by the action $(g \cdot f)(x) = f(xg)$ for all $x, g \in G$. The module $\mathrm{Ind}_H^G(A)$ is called the **coinduced module** from H to G.

2. **Induction:** The induction functor $\mathrm{ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ is defined by

$$A \mapsto \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$$

   This is called the **induced module** from H to G.

3. **Restriction:** The restriction functor $\mathrm{Res}_H^G : \mathrm{Mod}_G \to \mathrm{Mod}_H$ is defined by

$$A \mapsto \mathrm{Res}_H^G A = A \text{ (viewed as an } H\text{-module)}$$

4. A G-module is called **coinduced** if $A \cong \mathrm{Ind}_{\{e\}}^G X$ for some abelian group X. A direct factor of a coinduced G-module is called **relatively injective**.

5. A G-module is called **induced** if $A \cong \mathrm{ind}_{\{e\}}^G X$ for some abelian group X. A direct factor of an induced G-module is called **relatively projective**.

Exercise 9.2. If the index $[G : H] < \infty$, then $\mathrm{Ind}_H^G A \cong \mathrm{ind}_H^G A$. In particular, if the group G is finite, $|G| < \infty$, then the induced module is the same as the coinduced module, and the notions of relatively projective and relatively injective coincide.

Proposition 9.1 (**Frobenius Reciprocity**)**.** For an H-module A' and a G-module A, we have the following isomorphisms of abelian groups:

$$\mathrm{Hom}_H(\mathrm{Res}_H^G A, A') \cong \mathrm{Hom}_G(A, \mathrm{Ind}_H^G A')$$
$$\mathrm{Hom}_H(A', \mathrm{Res}_H^G A) \cong \mathrm{Hom}_G(\mathrm{ind}_H^G A', A)$$

Proof. For the first isomorphism:

$$\begin{aligned}\mathrm{Hom}_G(A, \mathrm{Ind}_H^G A') &= \mathrm{Hom}_G(A, \mathrm{Hom}_H(\mathbb{Z}[G], A')) \\ &= \{f : A \times G \to A' \mid f(ga, x) = f(a, xg) \quad \forall g, x \in G,\ \forall a \in A \\ &\qquad\qquad f(a, hx) = hf(a, x) \quad \forall h \in H\} \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}(A \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G], A') \\ &= \mathrm{Hom}_H(\mathrm{Res}_H^G A, A')\end{aligned}$$

For the second isomorphism:

$$\begin{aligned}\mathrm{Hom}_G(\mathrm{ind}_H^G A', A) &= \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A', A) \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}(A', A) \\ &= \mathrm{Hom}_H(A', \mathrm{Res}_H^G A)\end{aligned}$$

□

Remark: Take $A' = \mathrm{Res}_H^G A$. Then there is a natural G-module homomorphism

$$A \to \mathrm{Ind}_H^G \mathrm{Res}_H^G A = \mathrm{Hom}_H(\mathbb{Z}[G], A)$$

which sends an element $a \in A$ to the map $[g \mapsto ga]$. For example, if $H = \{e\}$, this gives the map $A \hookrightarrow \mathrm{Ind}_{\{e\}}^G A$.

Similarly, there is a natural H-module homomorphism

$$\mathrm{Res}_H^G \mathrm{Ind}_H^G A' \to A'$$

which sends an element $[f : G \to A']$ to $f(1)$.

Corollary 9.1. Injective (resp. projective) G-modules are always relatively injective (resp. projective).

Proof. **Claim:** For injective G-module A, it is a direct factor of a coinduced G-module $\mathrm{Ind}_{\{e\}}^G A$. For projective G-module A, it is a direct factor of an induced G-module $\mathrm{ind}_{\{e\}}^G A$.

For injective G-module A, consider the G-module homomorphism:

$$\begin{aligned}\iota : A &\to \mathrm{Ind}_{\{e\}}^G A \\ a &\mapsto [g \mapsto ga]\end{aligned}$$

is injective. Because A is injective G-module, there exists a G-module homomorphism $j : \mathrm{Ind}_{\{e\}}^G A \to A$ such that $j \circ \iota = \mathrm{id}_A$. Then:

$$\begin{aligned}\mathrm{Ind}_{\{e\}}^G A &\cong \ker(j) \oplus \mathrm{Im}(\iota) \\ &\cong \ker(j) \oplus A\end{aligned}$$

This shows that A is a direct factor of the coinduced G-module $\mathrm{Ind}_{\{e\}}^G A$.

For projective G-module A, consider the G-module homomorphism:

$$\begin{aligned}\pi : \mathrm{ind}_{\{e\}}^G A &\to A \\ [g \otimes a] &\mapsto ga\end{aligned}$$

is surjective. Because A is projective G-module, there exists a G-module homomorphism $s : A \to \mathrm{ind}_{\{e\}}^G A$ such that $\pi \circ s = \mathrm{id}_A$. Then:

$$\begin{aligned}\mathrm{ind}_{\{e\}}^G A &\cong \ker(\pi) \oplus \mathrm{Im}(s) \\ &\cong \ker(\pi) \oplus A\end{aligned}$$

This shows that A is a direct factor of the induced G-module $\mathrm{ind}_{\{e\}}^G A$. □

Corollary 9.2. Any G-module A can be embedded into the coinduced G-module $\mathrm{Ind}_{\{e\}}^G A$. Moreover, A is a direct factor of $\mathrm{Ind}_{\{e\}}^G A$ as a $\mathbb{Z}$-module.

Proof. The embedding is given by the natural G-module homomorphism

$$A \to \mathrm{Ind}_{\{e\}}^G A = \mathrm{Hom}(\mathbb{Z}[G], A)$$

which sends an element $a \in A$ to the map $[g \mapsto ga]$. We can define a retraction, which is a $\mathbb{Z}$-module homomorphism:

$$\begin{aligned}\mathrm{Ind}_{\{e\}}^G A &\to A \\ f &\mapsto f(1)\end{aligned}$$

This shows that the embedding is a split monomorphism of abelian groups. □

9.3 Group Cohomology and Homology

Fact: The category Mod_G has enough injective objects. (i.e., for any G-module A, there exists an injective G-module I and a monomorphism $A \hookrightarrow I$). Indeed, this holds for

the module category over any ring, Mod_R. The category also has enough projective objects (since free modules are projective).

In particular, for any G-module $A \in \mathrm{Mod}_G$, there exists an injective resolution: an exact sequence

$$0 \to A \to I^0 \to I^1 \to I^2 \to \dots$$

where all the modules I^n are injective G-modules.

For any functor $F : \mathrm{Mod}_G \to \mathcal{B}$ between abelian categories that is **covariant and left exact**, we can define its right derived functors R^iF:

$$(R^iF)(A) = H^i(F(I^\bullet))$$

For $i \geq 0$, we have $R^0F = F$.

Now consider the functor $F = (-)^G : \mathrm{Mod}_G \to \mathrm{Ab}$, where Ab is the category of abelian groups.

$$A \mapsto A^G = \{a \in A \mid ga = a \quad \forall g \in G\}$$

This is the functor of G-invariants.

Definition 9.6. The **group cohomology** of G with coefficients in a G-module A is defined as the right derived functors of the G-invariants functor:

$$H^i(G; A) := (R^iF)(A) \quad \text{for } i \geq 0.$$

Indeed, $H^i(G; A) = H^i(I^{\bullet,G})$, where $A \to I^\bullet$ is an injective resolution of A and $I^{\bullet,G}$ is the resulting complex of G-invariants. (**Note:** The sequence $\{I^{\bullet,G}\}$ must be a complex, but not necessarily exact).

Functoriality: A G-module homomorphism $\varphi : A \to B$ induces maps on cohomology:

$$\varphi_* : H^i(G; A) \to H^i(G; B)$$

This is because a map between modules can be lifted to a map between their injective resolutions. (**Note:** This is a property of injective resolutions in general, not specific to G-modules.)

$$\begin{array}{ccc} A & \longrightarrow & I^\bullet \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle f^\bullet} \\ B & \longrightarrow & J^\bullet \end{array}$$

Proposition 9.2 (**Properties of Group Cohomology**).

1. $H^0(G;A) = A^G$.
2. $H^i(G;A) = 0$ for all $i > 0$ if A is an injective G-module.
3. For any short exact sequence of G-modules $0 \to A \to B \to C \to 0$, we have a long exact sequence in cohomology:
$$0 \to A^G \to B^G \to C^G \to H^1(G;A) \to H^1(G;B) \to H^1(G;C) \to H^2(G;A) \to \dots$$
4. $H^i(G;\prod_j A_j) = \prod_j H^i(G;A_j)$ (as the direct product functor is exact).

Exercise 9.3.

1. If $[m] : A \to A$ is the multiplication-by-m map for some integer $m \in \mathbb{Z}$, then the induced map $[m]_* : H^i(G;A) \to H^i(G;A)$ is also multiplication by m.
2. If A is an m-torsion, then so is $H^i(G;A)$ for all $i \geq 0$.

Similarly, if $F : \mathrm{Mod}_G \to \mathcal{B}$ is an additive, covariant, and **right exact** functor, we can define its left derived functors L_iF for $i \geq 0$. Indeed, for any G-module $A \in \mathrm{Mod}_G$, we define

$$(L_iF)(A) = H_i(F(P_\bullet))$$

where $P_\bullet \to A$ is a projective resolution of A.

Consider the functor $F = (-)_G : \mathrm{Mod}_G \to \mathrm{Ab}$, which maps

$$A \mapsto A_G := A/I_GA$$

where I_G is the **augmentation ideal** of the group ring $\mathbb{Z}[G]$:

$$\begin{aligned} I_G &:= \ker(\epsilon : \mathbb{Z}[G] \to \mathbb{Z}) \quad \text{where } \epsilon\left(\sum a_g g\right) = \sum a_g \\ &= \left\{\sum a_g g \in \mathbb{Z}[G] \mid \sum a_g = 0\right\} \end{aligned}$$

The ideal I_G is generated by the elements $\{g - 1 \mid g \in G\}$. The module A_G is called the G-module of **co-invariants**.

Definition 9.7. The **group homology** of G with coefficients in A is defined as

$$H_i(G; A) := (L_iF)(A).$$

Proposition 9.3 (**Properties of Group Homology**).

1. $H_0(G; A) = A_G$.
2. $H_i(G; A) = 0$ for all $i > 0$ if A is a projective G-module.
3. For any short exact sequence of G-modules $0 \to A \to B \to C \to 0$, we have a long exact sequence in homology:
$$\cdots \to H_1(G; A) \to H_1(G; B) \to H_1(G; C) \to A_G \to B_G \to C_G \to 0$$
4. Homology commutes with direct sums.

We can also use projective resolutions to compute group cohomology $H^i(G; A)$. The G-invariants functor can be expressed using a Hom functor:

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

where $\mathbb{Z}$ is considered as a trivial G-module. The G-invariants functor $(-)^G$ is the functor $\mathrm{Hom}_G(\mathbb{Z}, -)$. Therefore, the group cohomology groups are the Ext groups in the category of G-modules:

$$H^i(G; A) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

To compute this, we take a projective resolution of $\mathbb{Z}$ as a G-module, $P_\bullet \to \mathbb{Z}$, and then

$$H^i(G; A) = H^i(\mathrm{Hom}_G(P_\bullet, A))$$

Similarly, for group homology, the G-coinvariants functor can be expressed using a tensor product:

$$A_G = A/I_GA \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$$

where $\mathbb{Z}$ is again a trivial G-module. The G-coinvariants functor $(-)_G$ is the functor $\mathbb{Z}\otimes_{\mathbb{Z}[G]}-$.

Therefore, the group homology groups are the Tor groups:

$$H_i(G; A) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

We will define a standard projective resolution of $\mathbb{Z}$ in the next lecture, denoted $P_\bullet \to \mathbb{Z}$, to compute $H^i(G; A)$. The n-th term in this resolution is given by

$$P_n = \mathbb{Z}[G^{n+1}]$$

9.4 Homework

Homework 9.1. The representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C})$ always factors through the Galois group of a finite Galois extension, $\mathrm{Gal}(L/K)$, for some field L.

Proof. There is a **Lemma**: If G is a matrix Lie group, with the Lie algebra $\mathfrak{g}$, then there exists an open neighborhood U of the identity element $0 \in \mathfrak{g}$, and an open neighborhood V of the identity element $e \in G$, such that the exponential map $\exp : \mathfrak{g} \to G$, when restricted to U, is a diffeomorphism onto V.

Consider:

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{C}) \xleftarrow{\exp} M_n(\mathbb{C})$$

And let $U \subset M_n(\mathbb{C})$ be an open neighborhood of 0 such that there exists $\varepsilon \in \mathbb{R}_{>0}$ such that:

$$U \subseteq B_\varepsilon(0) = \{X \in M_n(\mathbb{C}) \mid \|X\| < \varepsilon\}$$

$V \subseteq \mathrm{GL}_n(\mathbb{C})$ be an open neighborhood of I_n, such that $\exp|_U : U \to V$ is a diffeomorphism onto an open neighborhood V of $I_n \in \mathrm{GL}_n(\mathbb{C})$.

Consider the open set $\rho^{-1}(V) \subseteq \mathrm{Gal}(\overline{K}/K)$. It is well known that as a profinite group, $\mathrm{Gal}(\overline{K}/K)$ has a basis of open neighborhoods of the identity element $e \in \mathrm{Gal}(\overline{K}/K)$, consisting of open normal subgroups. We can find an open normal subgroup $N \trianglelefteq \mathrm{Gal}(\overline{K}/K)$,

$(\exp|_U)^{-1} \circ \rho(N)$ is a subgroup of $(M_n(\mathbb{C}), +)$. We **claim** that $\rho(N) \subseteq \ker \rho$. If not, there exists some $\sigma \in N$ such that $A := (\exp|_U)^{-1} \circ \rho(\sigma) \neq 0$. There exists some integer $m \in \mathbb{Z}_{>0}$ such that $\|mA\| > \varepsilon$, while $mA = (\exp|_U)^{-1} \circ \rho(\sigma^m) \in (\exp|_U)^{-1} \circ \rho(N) \subseteq U \subseteq B_\varepsilon(0)$, a contradiction!

Therefore, ρ factors through the finite quotient group $\mathrm{Gal}(\overline{K}/K)/N \cong \mathrm{Gal}(L/K)$, where $L = (\overline{K})^N$ is the fixed field of N. Because N is open normal and $\mathrm{Gal}(\overline{K}/K)$ is profinite,

$$[L : K] = [\mathrm{Gal}(\overline{K}/K) : N] < \infty$$

□

Homework 9.2. If the index $[G : H] < \infty$, then for a H-module A , $\mathrm{Ind}_H^G A \cong \mathrm{ind}_H^G A$.

Proof. We choose a set of representatives $\{g_1, g_2, \ldots, g_n\}$ of the right cosets of H in G:

$$G = \bigsqcup_{i=1}^{n} H g_i$$

where $n = [G : H]$. Then define a map Φ (so far depends on the choice of coset representatives):

$$\begin{aligned}\Phi : \mathrm{Hom}_H(\mathbb{Z}[G], A) &\to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \\ f &\mapsto \sum_{i=1}^{n} g_i^{-1} \otimes f(g_i)\end{aligned}$$

Obviously $\Phi(f + f') = \Phi(f) + \Phi(f')$, so Φ is a homomorphism of abelian groups. We need to check that Φ is a G-module homomorphism. For any $g \in G$:

$$\begin{aligned}\Phi(g \cdot f) &= \sum_{i=1}^{n} g_i^{-1} \otimes (g \cdot f)(g_i) \\ &= \sum_{i=1}^{n} g_i^{-1} \otimes f(g_i g) \\ &:= \sum_{i=1}^{n} g_i^{-1} \otimes f(h_i g_{\sigma(i)}) \quad \text{where } g_i g = h_i g_{\sigma(i)},\ h_i \in H \\ &= \sum_{i=1}^{n} g_i^{-1} \otimes h_i f(g_{\sigma(i)}) \\ &= \sum_{i=1}^{n} g_i^{-1} h_i \otimes f(g_{\sigma(i)}) \\ &= \sum_{i=1}^{n} g g_{\sigma(i)}^{-1} \otimes f(g_{\sigma(i)}) \\ &= g \cdot \Phi(f)\end{aligned}$$

Remark: We consider $\mathbb{Z}[G]$ as right $\mathbb{Z}[H]$-module when computing $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$.

We now construct the map Ψ: first for every element $x \in \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$ can be written as

$$\begin{aligned}x &:= \sum_{j=1}^{m} x_j \otimes a_j \\ &= \sum_{j=1}^{m} g_{\tau(j)}^{-1} h_j \otimes a_j \quad \text{where } h_j \in H \text{ such that } x_j^{-1} = h_j^{-1} g_{\tau(j)} \\ &= \sum_{j=1}^{m} g_{\tau(j)}^{-1} \otimes h_j a_j \\ &= \sum_{i=1}^{n} g_i^{-1} \otimes \sum_{\tau(j)=i} (h_j a_j)\end{aligned}$$

So every $x \in \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$ can be uniquely written as:

$$x = \sum_{i=1}^{n} g_i^{-1} \otimes a_i' \quad \text{where } a_i' = \sum_{\tau(j)=i} (h_j a_j) \in A$$

(Uniqueness comes from $\mathbb{Z}[G] = \bigoplus_{i=1}^{n} g_i \cdot \mathbb{Z}[H]$ as right $\mathbb{Z}[H]$-modules.)

Then we can define:

$$\Psi : \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \to \mathrm{Hom}_H(\mathbb{Z}[G], A)$$
$$x = \sum_{i=1}^{n} g_i^{-1} \otimes a_i' \mapsto (f_x : hg_i \mapsto ha_i')$$

f_x is obviously H-module homomorphism and Ψ is obviouly a homomorphism of abelian groups. We need to check that Ψ is a G-module homomorphism:

$$\begin{aligned}
\Psi(g \cdot x) &= \Psi\left(\sum_{i=1}^{n} (gg_i^{-1}) \otimes a_i'\right) \\
&= \Psi\left(\sum_{i=1}^{n} g_{\sigma(i)}^{-1} h_i \otimes a_i'\right) \quad \text{where } gg_i^{-1} = g_{\sigma(i)}^{-1} h_i,\ h_i \in H \\
&= \Psi\left(\sum_{i=1}^{n} g_{\sigma(i)}^{-1} \otimes h_i a_i'\right) \\
&= (f_{g\cdot x} : hg_{\sigma(i)} \mapsto h(h_i a_i'))
\end{aligned}$$

On the other hand:

$$(g \cdot \Psi(x))(g_{\sigma(i)}) = f_x(g_{\sigma(i)} g) = f_x(h_i g_i) = h_i a_i'$$

So $\Psi(g \cdot x) = g \cdot \Psi(x)$.

It is easy to check that Φ and Ψ are inverses of each other, i.e. $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. Therefore, we have proved the isomorphism. □

Remark: Actually the isomorphism does not depend on the choice of coset representatives.

Homework 9.3. Let G be a finite group. Let A and B be G-modules.

(a) Assume that B is induced. Show that the G-module $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is induced;

(b) Assume that A is a projective G-module. Show that $A \otimes_{\mathbb{Z}} B$ is a relatively injective G-module.

Proof of (a). Since B is induced, there exists some abelian group X such that $B = \operatorname{ind}_{\{e\}}^{G} X$. We **claim** that:

$$\operatorname{Hom}_{\mathbb{Z}}(A, \operatorname{ind}_{\{e\}}^{G} X) \cong \operatorname{ind}_{\{e\}}^{G} \operatorname{Hom}_{\mathbb{Z}}(A, X)$$

Because G is finite, we will use the isomorphism between induced and coinduced modules:

$$\begin{aligned}
\operatorname{Hom}_{\mathbb{Z}}(A, \operatorname{ind}_{\{e\}}^{G} X) &\cong \operatorname{Hom}_{\mathbb{Z}}(A, \operatorname{Ind}_{\{e\}}^{G} X) \\
&= \operatorname{Hom}_{\mathbb{Z}}(A, \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)) \\
&\cong \operatorname{Hom}_{\mathbb{Z}}(A \otimes_{\mathbb{Z}} \mathbb{Z}[G], X) \\
&\cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} A, X) \\
&\cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \operatorname{Hom}_{\mathbb{Z}}(A, X)) \\
&= \operatorname{Ind}_{\{e\}}^{G} \operatorname{Hom}_{\mathbb{Z}}(A, X) \\
&\cong \operatorname{ind}_{\{e\}}^{G} \operatorname{Hom}_{\mathbb{Z}}(A, X)
\end{aligned}$$

□

Proof of (b). Since A is a projective G-module, it is a direct factor of an free G-module $\mathbb{Z}[G]^{(I)}$ for some index set I, i.e.:

$$A \oplus C \cong \mathbb{Z}[G]^{(I)} \quad \text{for some } G\text{-module } C$$

Then:

$$(A \otimes_{\mathbb{Z}} B) \oplus (C \otimes_{\mathbb{Z}} B) \cong (\mathbb{Z}[G]^{(I)}) \otimes_{\mathbb{Z}} B \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} (\mathbb{Z})^{(I)} \otimes_{\mathbb{Z}} B \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} (B)^{(I)}$$

Hence, $A \otimes_{\mathbb{Z}} B$ is a direct factor of the induced G-module $\operatorname{ind}_{\{e\}}^{G}(B)^{(I)}$. So $A \otimes_{\mathbb{Z}} B$ is relatively projective. Because G is finite, $A \otimes_{\mathbb{Z}} B$ is also relatively injective. □

Homework 9.4. Let A be a G-module. Let $m \in \mathbb{N}$.

(a) If $[m] : A \to A$ denotes the multiplication by m. Then $[m]_* : H^i(G, A) \to H^i(G, A)$ is also the multiplication by m for all $i \geq 0$.

(b) If A is m-torsion, then $H^i(G, A)$ is also m-torsion $\forall i \geq 0$.

Proof of (a). The cohomology groups are the right derived functors of the G-invariants functor, $F = (-)^G$, computed via an injective resolution $A \to I^\bullet$. The map $[m]_A$ lifts to a chain map $[m]_{I^\bullet} : I^\bullet \to I^\bullet$ where each component is also multiplication by m. Applying the functor F gives a chain map on the complex of invariants, $([m]_{I^\bullet})^G : (I^\bullet)^G \to (I^\bullet)^G$, which is simply multiplication by m on each term because it is just the restriction of $[m]_{I^\bullet}$ to the G-invariant elements.

The map induced on cohomology sends a class $[c]$ (represented by a cocycle $c \in (I^i)^G$) to the class $[m \cdot c]$. Since the cohomology groups are abelian groups, this is equal to $m \cdot [c]$. Therefore, the induced map $([m]_A)_*$ is precisely multiplication by m on the abelian group $H^i(G, A)$. □

Proof of (b). A G-module A is m-torsion if the multiplication-by-m map, $[m]_A : A \to A$, is the zero homomorphism.

From part (a), we know that the map induced on cohomology, $([m]_A)_*$, is multiplication by m. Functoriality implies that if the original map is zero, the induced map on cohomology is also zero. Since $[m]_A$ is the zero map, its induced map $([m]_A)_*$ must also be the zero map on $H^i(G, A)$.

$$([m]_A)_* = 0_{H^i(G,A) \to H^i(G,A)}$$

This means that for any element $\alpha \in H^i(G, A)$, we have $m \cdot \alpha = 0$. By definition, this shows that the group $H^i(G, A)$ is an m-torsion group for all $i \geq 0$. □

10 2025.11.13

Let G be a group and A be a G-module. We have $A^G = \mathrm{Hom}_G(\mathbb{Z}, A)$ and

$$H^i(G; A) = H^i(\mathrm{Hom}_G(P_\bullet, A))$$

where $P_\bullet \to \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$ as a G-module.

10.1 Cochains

Definition 10.1. Let $P_i := \mathbb{Z}[G^{i+1}]$, where G acts on G^{i+1} via the diagonal action on the left.

Remark: The modules P_i are free G-modules, and therefore projective. Indeed, a basis can be chosen to be the set of representatives for each orbit of the action of G on G^{i+1}.

Definition 10.2. The augmentation map $d_0 : P_0 = \mathbb{Z}[G] \to \mathbb{Z}$ is defined by

$$\sum a_g g \mapsto \sum a_g$$

The differential maps $d_i : P_i = \mathbb{Z}[G^{i+1}] \to P_{i-1} = \mathbb{Z}[G^i]$ are defined on the basis elements $(g_0, \ldots, g_i) \in G^{i+1}$ by

$$(g_0, \ldots, g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_i)$$

where $\hat{g_j}$ denotes that the j-th component is omitted.

We can check that the sequence

$$\ldots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0$$

is exact. It is called the **standard resolution** (or bar resolution) of $\mathbb{Z}$.

Using this resolution, the cohomology is computed as

$$H^i(G; A) = H^i(\mathrm{Hom}_G(P_\bullet, A))$$

The group of i-cochains is $\mathrm{Hom}_G(P_i, A)$. We have an isomorphism:

$$\mathrm{Hom}_G(P_i, A) = \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A) \cong \{f : G^{i+1} \to A \mid f(gg_0, \ldots, gg_i) = gf(g_0, \ldots, g_i)\}$$

Such a function f is called a **homogeneous i-cochain**.

The differential maps $d_i : P_i \to P_{i-1}$ from the projective resolution induce coboundary maps $d^i : \mathrm{Hom}_G(P_{i-1}, A) \to \mathrm{Hom}_G(P_i, A)$.

Definition 10.3. The elements in the kernel of these maps, $\ker(d^{i+1})$, are called **homogeneous i-cocycles**. The elements in the image of these maps, $\mathrm{Im}(d^i)$, are called **homogeneous i-coboundaries**.

There is a well-known isomorphism between the homogeneous and inhomogeneous cochain complexes.

$$\begin{array}{ccc}
\{\text{homogeneous } i\text{-cochains, } f : G^{i+1} \to A\} & \longleftrightarrow & \{\text{inhomogeneous } i\text{-cochains, } f : G^i \to A\} := C^i(G, A) \\
\cup & & \\
\{\text{homogeneous } i\text{-cocycles}\} & \longleftrightarrow & \{\text{inhomogeneous } i\text{-cocycles}\} := Z^i(G, A) \\
\cup & & \\
\{\text{homogeneous } i\text{-coboundaries}\} & \longleftrightarrow & \{\text{inhomogeneous } i\text{-coboundaries}\} := B^i(G, A)
\end{array}$$

By:

$$f \mapsto \tilde{f} \quad \text{where } \tilde{f}(g_1, \ldots, g_i) = f(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_i)$$

The coboundary map for the inhomogeneous complex $d : C^i(G, A) \to C^{i+1}(G, A)$ is given as follows:

For $i = 0$: $d : C^0(G, A) = A \to C^1(G, A)$.

$$a \mapsto [g \mapsto ga - a]$$

For $i \geq 1$: $d : C^i(G, A) \to C^{i+1}(G, A)$. For a function $f : G^i \to A$,

$$\begin{aligned}
(df)(g_1, \ldots, g_{i+1}) = g_1 f(g_2, \ldots, g_{i+1}) &+ \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) \\
&+ (-1)^{i+1} f(g_1, \ldots, g_i).
\end{aligned}$$

Example 10.1. A **1-coboundary** is a function $f : G \to A$ of the form $g \mapsto ga - a$ for

some $a \in A$. A **1-cocycle** is a function $f : G \to A$ such that $df = 0$. The condition is:

$$(df)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0$$
$$\text{i.e., } f(g_1 g_2) = g_1 f(g_2) + f(g_1) \quad \forall g_1, g_2 \in G.$$

A 1-cocycle is also called a **crossed homomorphism** or **twisted homomorphism**. In particular, if A is a trivial G-module, the 1-cocycle condition becomes $f(g_1 g_2) = f(g_1) + f(g_2)$. In this case,

$$H^1(G, A) = \frac{\{\text{1-cocycles}\}}{\{\text{1-coboundaries}\}} = \text{Hom}(G, A)$$

since the only 1-coboundary is the zero map.

Definition 10.4. Let A be a G-module. A **G-torsor over A** is a G-set X with an A-action $A \times X \to X$ such that:

1. The action of A on X is simply transitive, denoted by:
$$+ : A \times X \to X : (a, x) \mapsto a + x$$
2. For all $g \in G$, $x \in X$, and $a \in A$, the actions are compatible: $g \cdot (a + x) = (g \cdot a) + (g \cdot x)$.

Exercise 10.1. Show that $H^1(G, A)$ classifies the isomorphism classes of G-torsors over A.

10.2 Change of groups

Let $f : G' \to G$ be a group homomorphism. Any G-module A can be viewed as a G'-module via restriction of scalars. Let $f^*A \in \text{Mod}_{G'}$ denote the module A with the G'-action given by $g' \cdot a = f(g') \cdot a$. For $i = 0$, we have $H^0(G, A) = A^G$ and $(f^*A)^{G'} = H^0(G', f^*A)$. We have a natural transformation of functors:

$$H^0(G, -) \to H^0(G', f^*(-))$$

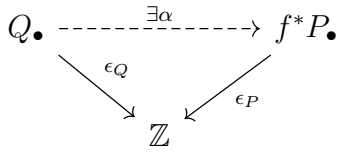
This gives rise to maps $f^* : H^i(G, -) \to H^i(G', f^*(-))$.

Remark: Indeed, the map f^* can be explained as follows. Let $P_\bullet \to \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ as a G-module. Let $Q_\bullet \to \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ as a G'-module.

The map f^* on cohomology is the composition

$$H^i(\mathrm{Hom}_G(P_\bullet, -)) \to H^i(\mathrm{Hom}_{G'}(f^*P_\bullet, f^*(-))) \to H^i(\mathrm{Hom}_{G'}(Q_\bullet, f^*(-)))$$

The second map is induced by a chain map $f^*P_\bullet \to Q_\bullet$ lifting the identity map on $\mathbb{Z}$, which exists by the properties of projective resolutions.



Definition 10.5. Let A be a G-module and A' be a G'-module. A homomorphism of G'-modules $u : f^*A \to A'$ induces a map

$$H^i(G; A) \xrightarrow{f^*} H^i(G'; f^*A) \xrightarrow{u_*} H^i(G'; A')$$

Definition 10.6.

1. Let A be a G-module and let $H \subseteq G$ be a subgroup. The inclusion map $i : H \hookrightarrow G$ induces the **restriction homomorphism**:

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

2. Let H be a normal subgroup of G. Let $A \in \mathrm{Mod}_G$ be such that $A^H \in \mathrm{Mod}_{G/H}$ (i.e., the action of G on A preserves the subgroup of H-invariants). The projection map $p : G \to G/H$ induces the **inflation homomorphism**:

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

Remark: The restriction and inflation maps have a very simple expression on the level of cocycles.

- **Restriction:** $\mathrm{Res} : Z^i(G, A) \to Z^i(H, A)$. A cocycle $f : G^i \to A$ is simply restricted to the subgroup H^i, i.e., $\mathrm{Res}(f) = f|_{H^i}$.
- **Inflation:** The inflation map on cocycles is given by

$$\mathrm{Inf} : Z^i(G/H, A^H) \to Z^i(G, A)$$
$$[f : (G/H)^i \to A^H] \mapsto [G^i \to (G/H)^i \xrightarrow{f} A^H \hookrightarrow A]$$

We have $\mathrm{Res} \circ \mathrm{Inf} = 0$.

Recall: By Frobenius reciprocity, for any H-module A, there is a natural homomorphism $u : \mathrm{Res}^G_H \mathrm{Ind}^G_H A \to A$ by $[f : \mathbb{Z}[G] \to A] \mapsto f(e_G)$. So we have a map:

$$H^i(G, \mathrm{Ind}^G_H A) \xrightarrow{\mathrm{Res}} H^i(H, \mathrm{Res}^G_H \mathrm{Ind}^G_H A) \xrightarrow{u_*} H^i(H, A)$$

Theorem 10.1 (**Shapiro's Lemma**)**.** Let $f : H \to G$ be a group homomorphism and let A be an H-module. Then the map

$$H^i(G, \mathrm{Ind}^G_H A) \xrightarrow{\cong} H^i(H, A)$$

induced by the composition $\mathrm{Res} \circ u$ is an isomorphism.

Proof. For the case $i = 0$:

$$\begin{aligned} H^0(G, \mathrm{Ind}^G_H A) &= (\mathrm{Ind}^G_H A)^G \\ &= \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}^G_H A) \\ &\cong \mathrm{Hom}_H(\mathrm{Res}^G_H \mathbb{Z}, A) \quad \text{(by Frobenius reciprocity)} \\ &\cong \mathrm{Hom}_H(\mathbb{Z}, A) \\ &= A^H = H^0(H, A) \end{aligned}$$

For $i > 0$: Let $A \to I^\bullet$ be an injective resolution of A as an H-module. The functor Ind^G_H maps this to an injective resolution $\mathrm{Ind}^G_H A \to \mathrm{Ind}^G_H I^\bullet$ of $\mathrm{Ind}^G_H A$ as a G-module, because Ind^G_H is an exact functor that preserves injective objects. The functor $\mathrm{Ind}^G_H(-) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], -)$ is exact because $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module.

This implies:

$$\begin{array}{ccc} H^i(G, \mathrm{Ind}^G_H A) & \xrightarrow{\cong} & H^i(H, A) \\ \| & & \| \\ H^i((\mathrm{Ind}^G_H I^\bullet)^G) & \to & H^i((I^\bullet)^H) \end{array}$$

It remains to show that $(\mathrm{Ind}^G_H I^j)^G \cong (I^j)^H$ for all j.

$$H^0(G, \mathrm{Ind}^G_H I^j) \cong H^0(H, I^j) \quad \text{(by Frobenius reciprocity)}$$

□

Corollary 10.1. If a G-module A is relatively injective (i.e., A is a direct factor of $\mathrm{Ind}_{\{e\}}^{G} X$ for some abelian group X), then $H^i(G, A) = 0$ for all $i > 0$.

Proof. It suffices to show this for $A = \mathrm{Ind}_{\{e\}}^{G} X$. Then by Shapiro's Lemma,

$$H^i(G, A) = H^i(G, \mathrm{Ind}_{\{e\}}^{G} X) \cong H^i(\{e\}, X) = 0 \quad \forall i > 0.$$

$= 0$ is because the functor $(-)^{\{e\}}$ is trivial. □

Corollary 10.2 (Dimension Shifting). Let $0 \to A \to I \to B \to 0$ be an exact sequence of G-modules, where I is relatively injective. Then the connecting homomorphism $H^i(G, B) \to H^{i+1}(G, A)$ is surjective for $i = 0$ and is an isomorphism for $i \geq 1$.

Proposition 10.1. Let G be a finite group. Let $\{A_j\}_{j \in J}$ be an inductive system (direct system) of G-modules. Let $A = \varinjlim A_j$. Then for $i \geq 0$,

$$H^i(G, A) = \varinjlim_j H^i(G, A_j).$$

Proof of Proposition. For $i = 0$, the result is obvious. For $i \geq 1$, we use dimension shifting. For each j, we have a short exact sequence

$$0 \to A_j \to \mathrm{Ind}_{\{e\}}^{G} A_j \to B_j \to 0$$

Since the direct limit functor $\varinjlim_j$ is exact, we get an exact sequence

$$0 \to \varinjlim_j A_j \to \varinjlim_j \mathrm{Ind}_{\{e\}}^{G} A_j \to \varinjlim_j B_j \to 0$$

which is $0 \to A \to \mathrm{Ind}_{\{e\}}^{G} A \to B \to 0$. See detail in appendix. (Remark: G should be finite here to ensure that $\mathrm{Ind}_{\{e\}}^{G}$ commutes with direct limits.)

For $i > 0$, from the dimension shifting, we have isomorphisms $H^i(G; B_j) \cong H^{i+1}(G; A_j)$, hence:

$$\varinjlim_j H^i(G; B_j) \cong \varinjlim_j H^{i+1}(G; A_j)$$

If we proved that $\varinjlim_j H^i(G; B_j) \cong H^i(G; B)$, then also by dimension shifting we would have

$$H^{i+1}(G; A) \cong H^i(G; B) \cong \varinjlim_j H^i(G; B_j) \cong \varinjlim_j H^{i+1}(G; A_j)$$

and the result would follow by induction. So it remains to show that $\varinjlim_j H^i(G; A_j) \cong H^i(G; A)$ for $i = 0, 1$.

For $i = 0$, it suffices to show:

$$(\varinjlim_j A_j)^G \cong \varinjlim_j (A_j)^G$$
$$\mathrm{Hom}_G(\mathbb{Z}, \varinjlim_j A_j) \cong \varinjlim_j \mathrm{Hom}_G(\mathbb{Z}, A_j)$$

See detail in appendix.

For $i = 1$, we use the exact sequence

$$H^0(G, \mathrm{Ind}_{\{e\}}^G A_j) \to H^0(G, B_j) \to H^1(G, A_j) \to 0$$

Taking direct limits, we get an exact sequence

$$\varinjlim_j H^0(G, \mathrm{Ind}_{\{e\}}^G A_j) \to \varinjlim_j H^0(G, B_j) \to \varinjlim_j H^1(G, A_j) \to 0$$

Compare with the exact sequence:

$$H^0(G, \mathrm{Ind}_{\{e\}}^G A) \to H^0(G, B) \to H^1(G, A) \to 0$$

And there is natural morphism between these two exact sequences. By the case $i = 0$, we have $\varinjlim_j H^0(G, \mathrm{Ind}_{\{e\}}^G A_j) \cong H^0(G, \mathrm{Ind}_{\{e\}}^G A)$. Also, we have $\varinjlim_j H^0(G, B_j) \cong H^0(G, B)$ by the case $i = 0$. Hence, we will have:

$$\varinjlim_j H^1(G, A_j) \cong H^1(G, A)$$

□

10.3 Inflation-Restriction exact sequence

Theorem 10.2. Let H be a normal subgroup of G, and let A be a G-module. Then the following sequence is exact:

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

Proof. We have already shown that $\text{Res} \circ \text{Inf} = 0$.

Recall that a 1-cocycle is a map $f : G \to A$ such that $f(g_1g_2) = g_1f(g_2) + f(g_1)$. A 1-coboundary is a map of the form $f(g) = ga - a$ for some $a \in A$. Let $[f] \in \ker(\text{Inf})$, where $f \in Z^1(G/H, A^H)$.

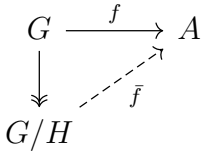
We want to show that $f \in B^1(G/H, A^H)$, i.e., there exists $a \in A^H$ such that $f(gH) = (gH)a - a$ for all $gH \in G/H$. The inflation map sends a cocycle $f : (G/H)^i \to A^H$ to the composition $G^i \to (G/H)^i \xrightarrow{f} A^H \hookrightarrow A$. The map on the 1-coboundary $g \mapsto ga - a$ for some $a \in A$ is zero. We want to show that $a \in A^H$. $0 = f(h) = ha - a \implies ha = a$. This holds for all $h \in H$, so $a \in A^H$.

Now we show $\ker(\text{Res}) \subseteq \text{Im}(\text{Inf})$. Let $[f] \in \ker(\text{Res})$, where $f \in Z^1(G, A)$. This means that the restriction of f to H, $f|_H$, is a 1-coboundary in $B^1(H, A)$. So, $f(h) = ha - a$ for some $a \in A$. We can modify the cocycle f by a coboundary without changing its cohomology class. Let $f_a(g) = ga - a$. Consider the new cocycle $f' = f - f_a$. Then $f'|_H = f|_H - f_a|_H = (ha - a) - (ha - a) = 0$. Without loss of generality, we can assume $f|_H = 0$.

The 1-cocycle condition for f is $f(gh) = gf(h) + f(g)$ for all $g \in G, h \in H$. Since $f(h) = 0$, this simplifies to $f(gh) = f(g)$. This shows that the function $f : G \to A$ is constant on the left cosets of H, and therefore factors through the quotient G/H. Let's check the image. Because H is normal, For any $g \in G, h \in H$, there exists $h' \in H$ such that $hg = gh'$. So:

$$f(g) = f(gh') = f(hg) = hf(g) + f(h) = hf(g) + 0 = hf(g)$$

So $f(g)$ must be in the subgroup of H-invariants, A^H. The map $f : G \to A$ factors through G/H to a map $\bar{f} : G/H \to A^H$.



This is what we proved. Then $f = \text{Inf}(\bar{f})$, so $[f] \in \text{Im}(\text{Inf})$.

□

Theorem 10.3. Let H be a normal subgroup of G and let A be a G-module such that $H^i(H, A) = 0$ for all $1 \leq i \leq n-1$. Then the sequence

$$0 \to H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A)$$

is exact.

Corollary 10.3. Under the same hypotheses, the inflation map $\text{Inf} : H^i(G/H, A^H) \to H^i(G, A)$ is an isomorphism for all $1 \leq i \leq n-1$.

Proof of Theorem. We proved the case $n = 1$ already. For $n \geq 2$, we prove by induction on n by using dimension shifting.

Consider the short exact sequence of G-modules

$$0 \to A \to \text{Ind}_{\{e\}}^G A \to B \to 0$$

This gives a long exact sequence in cohomology. Since $\text{Ind}_{\{e\}}^G A$ is relatively injective, its higher cohomology vanishes.

$$\cdots \to H^i(G, \text{Ind}_{\{e\}}^G A) \to H^i(G, B) \to H^{i+1}(G, A) \to H^{i+1}(G, \text{Ind}_{\{e\}}^G A) \to \dots$$

For $i \geq 1$, this gives an isomorphism $H^i(G, B) \cong H^{i+1}(G, A)$.

By the condition: we have the short exact sequence of H-invariants for the sequence of G-modules:

$$0 \to A^H \to (\text{Ind}_{\{e\}}^G A)^H \to B^H \to H^1(H, A) = 0$$

We have $(\text{Ind}_{\{e\}}^G A)^H = \text{Hom}_H(\mathbb{Z}, \text{Ind}_{\{e\}}^G A) \cong \text{Hom}_G(\mathbb{Z}[G/H], A) = \text{Ind}_{\{e\}}^{G/H} A$, which is a coinduced G/H-module. This implies $H^i(G/H, B^H) \cong H^{i+1}(G/H, A^H)$ for all $i \geq 1$.

Claim: $\text{Ind}_{\{e\}}^G A$ is a coinduced module as an H-module. Since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module, we can write $\mathbb{Z}[G] \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}} M$ for some abelian group M.

$$\begin{aligned}
\text{Ind}_{\{e\}}^G A &= \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \\
&\cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[H] \otimes_{\mathbb{Z}} M, A) \quad (\text{as } H\text{-modules}) \\
&\cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], \text{Hom}_{\mathbb{Z}}(M, A)) \\
&= \text{Ind}_{\{e\}}^H(\text{Hom}_{\mathbb{Z}}(M, A))
\end{aligned}$$

This shows that $\text{Ind}_{\{e\}}^G A$ is a coinduced H-module. Therefore, its higher H-cohomology vanishes: $H^i(H, \text{Ind}_{\{e\}}^G A) = H^i(H, \text{Ind}_{\{e\}}^H(\text{Hom}_{\mathbb{Z}}(M, A))) = 0$ for $i \geq 1$.

The long exact sequence for H-cohomology then gives $H^i(H, B) \cong H^{i+1}(H, A)$ for all $i \geq 1$. In particular, since $H^i(H, A) = 0$ for $1 \leq i \leq n-1$ by hypothesis, it follows that $H^i(H, B) = 0$ for $1 \leq i \leq n-2$.

We can now apply the induction hypothesis to the module B. The inflation-restriction sequence for H^{n-1} is exact:

$$0 \to H^{n-1}(G/H, B^H) \xrightarrow{\text{Inf}} H^{n-1}(G, B) \xrightarrow{\text{Res}} H^{n-1}(H, B)$$

Using the dimension shifting isomorphisms, this becomes:

$$0 \to H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A)$$

□

Remark: These two theorems could also be proved by the Hochschild-Serre spectral sequence. For the functor sequence $\text{Mod}_G \to \text{Mod}_{G/H} \to \text{Ab}$ where the first arrow is $A \mapsto A^H$ and the second is $M \mapsto M^{G/H}$, the spectral sequence has $E_2^{p,q} = H^p(G/H, H^q(H, A))$ and converges to $H^{p+q}(G, A)$.

10.4 Corestriction

Now suppose $[G : H] < \infty$. In this case, we want to define the corestriction map $\text{Cor} : H^i(H, A) \to H^i(G, A)$ for all $i \geq 0$.

For $i = 0$: $\text{Cor} : H^0(H, A) \to H^0(G, A)$. This is the norm map $N_{G/H}$:

$$\begin{aligned} A^H &\to A^G \\ a &\mapsto \sum_{g \in G/H} ga \end{aligned}$$

For general i: Let $P_\bullet \to \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ as a G-module. It is also a projective resolution of $\mathbb{Z}$ as an H-module (since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module).

$$\begin{aligned} H^i(H, A) &= H^i(\text{Hom}_H(P_\bullet, A)) \\ H^i(G, A) &= H^i(\text{Hom}_G(P_\bullet, A)) \end{aligned}$$

The corestriction map is induced by the trace map $N_{G/H} : \text{Hom}_H(P_i, A) \to \text{Hom}_G(P_i, A)$.

Another way to define corestriction: Since $[G : H] < \infty$, we have $\text{Ind}_H^G \cong \text{ind}_H^G$. By Frobenius reciprocity, there is a natural G-homomorphism (the trace map):

$$u : \text{Ind}_H^G \text{Res}_H^G A = \text{ind}_H^G \text{Res}_H^G A \to A$$

The corestriction map is the composition:

$$\begin{array}{ccc} H^i(H, \operatorname{Res}^G_H A) & \longrightarrow & H^i(G, A) \\ \downarrow \simeq & \nearrow_{u} & \\ H^i(G, \operatorname{Ind}^G_H \operatorname{Res}^G_H A) & & \end{array}$$

The vertical map is an isomorphism by Shapiro's Lemma.

Theorem 10.4. Let $[G : H] = m$. Then for all $i \geq 0$, the composition

$$H^i(G, A) \xrightarrow{\text{Res}} H^i(H, A) \xrightarrow{\text{Cor}} H^i(G, A)$$

is multiplication by m.

Proof. For $i = 0$: The composition is $A^G \xrightarrow{\text{Res}} A^H \xrightarrow{\text{Cor}} A^G$. An element $a \in A^G$ is mapped to $a \in A^H$, which is then mapped by the norm $N_{G/H}$ to $\sum_{g \in G/H} g \cdot a = \sum_{g \in G/H} a = ma$.

For the general case, we use dimension shifting. Consider the exact sequence of G-modules

$$0 \to A \to \operatorname{Ind}^G_{\{e\}} A \to B \to 0$$

This gives a commutative diagram with exact rows for $i \geq 1$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^i(G, B) & \longrightarrow & H^{i+1}(G, A) & \longrightarrow & 0 \\ & & \downarrow \text{Res} & & \downarrow \text{Res} & & \\ 0 & \longrightarrow & H^i(H, B) & \longrightarrow & H^{i+1}(H, A) & \longrightarrow & 0 \\ & & \downarrow \text{Cor} & & \downarrow \text{Cor} & & \\ 0 & \longrightarrow & H^i(G, B) & \longrightarrow & H^{i+1}(G, A) & \longrightarrow & 0 \end{array}$$

The result follows by induction. It remains to prove the case $i = 1$.

For $i = 1$, similarly we have:

$$\begin{array}{ccccccc} \dots & \longrightarrow & H^0(G, B) & \twoheadrightarrow & H^1(G, A) & \longrightarrow & \dots \\ & & \downarrow \text{Res} & & \downarrow \text{Res} & & \\ \dots & \longrightarrow & H^0(H, B) & \twoheadrightarrow & H^1(H, A) & \longrightarrow & \dots \\ & & \downarrow \text{Cor} & & \downarrow \text{Cor} & & \\ \dots & \longrightarrow & H^0(G, B) & \twoheadrightarrow & H^1(G, A) & \longrightarrow & \dots \end{array}$$

We have already proved the case $i = 0$, i.e. the left vertical composition is multiplication by m. By the surjectivity of the horizontal maps, the right vertical composition is also multiplication by m. □

Corollary 10.4. If $|G| = m$, and A is a G-module, then the cohomology groups $H^i(G, A)$ are m-torsion for all $i \geq 1$.

Proof. Apply the theorem to the case where $H = \{e\}$. The group $H^i(\{e\}, A)$ is the cohomology of the trivial group, which is 0 for $i \geq 1$. The composition $\mathrm{Res} \circ \mathrm{Cor}$ maps $H^i(G, A) \to H^i(\{e\}, A) \to H^i(G, A)$. Since the middle group is zero, the composition is the zero map. But we also know this map is multiplication by $m = |G|$. Therefore, multiplication by m on $H^i(G, A)$ is the zero map, which means the group is m-torsion. □

Corollary 10.5. Let $|G| < \infty$ and let $A \in \mathrm{Mod}_G$ be a G-module of finite type. Then the cohomology groups $H^i(G, A)$ are finite for all $i > 0$.

Proof. As $H^i(G, A)$ is $|G|$-torsion, it suffices to show that $H^i(G, A)$ are finitely generated as abelian groups. We have $H^i(G, A) = Z^i(G, A)/B^i(G, A)$. The group of cocycles $Z^i(G, A)$ is a subgroup of the group of all maps from G^i to A, $Z^i(G, A) \subseteq \mathrm{Map}(G^i, A)$. Since A is a finitely generated $\mathbb{Z}[G]$-module and G is finite, it is also a finitely generated $\mathbb{Z}$-module. Therefore, $\mathrm{Map}(G^i, A)$ is a finitely generated $\mathbb{Z}$-module. Submodules of finitely generated $\mathbb{Z}$-modules are finitely generated. Thus $Z^i(G, A)$ is finitely generated, and so is its quotient $H^i(G, A)$. □

Definition 10.7. For an abelian group A and a prime number p, the **p-primary component** of A is the subgroup of A consisting of all elements killed by a power of p.

Remark: If $|A| < \infty$, then $A(p)$ is the Sylow p-subgroup of A.

Corollary 10.6. Let G be a finite group. Let G_p be a Sylow p-subgroup of G. Then for any G-module A, the restriction map $\mathrm{Res} : H^i(G, A) \to H^i(G_p, A)$ is injective on the p-primary component of $H^i(G, A)$.

Proof. Let $m = [G : G_p]$. Then $p \nmid m$. The composition $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by m. The map $[m] : H^i(G, A)(p) \to H^i(G, A)(p)$ is an isomorphism. Since $[m] = \mathrm{Cor} \circ \mathrm{Res}$, this implies that the map Res must be injective on $H^i(G, A)(p)$. □

10.5 Homework

Homework 10.1. Let G be a finite group. Let $\mathbb{Q}$ be the trivial G-module. Show that $H^i(G, \mathbb{Q}) = 0$ for all $i > 0$.

Proof. From **Corollary 10.4**, denote $|G| = m$, we know that $H^i(G, \mathbb{Q})$ is m-torsion for all $i > 0$. For any $[c] \in H^i(G, \mathbb{Q})$, where $c \in Z^i(G, \mathbb{Q})$ is a cocycle representing the cohomology class $[c]$, we have $m[c] = 0$. This means that there exists a cochain $b \in C^{i-1}(G, \mathbb{Q})$ such that $mc = d^i(b)$. Note that b is of the form $b : G^{i-1} \to \mathbb{Q}$. Define a new cochain $b' : G^{i-1} \to \mathbb{Q}$ by

$$b'(g_1, g_2, \ldots, g_{i-1}) = \frac{1}{m} b(g_1, g_2, \ldots, g_{i-1})$$

Then we have $c = d^i(b')$. This shows that $[c] = 0$ in $H^i(G, \mathbb{Q})$. So $H^i(G, \mathbb{Q}) = 0$ for all $i > 0$. □

Homework 10.2. Let G be a group and A be a G-module. Let $t \in G$. Let $G' = G$ and $A' = A$. Let $f : G' \to G, g \mapsto t^{-1}gt$. Then $u : f^*A \to A', a \mapsto ta$ is a G'-homomorphism. It induces homomorphisms $\sigma_t : H^n(G, A) \to H^n(G, A)$ for $n \geq 0$. Show that σ_t are identity.

Proof. The σ_t comes from:

$$H^n(G, A) \xrightarrow{f^*} H^n(G', f^*A) \xrightarrow{u_*} H^n(G', A')$$

Note that for an injective resolution $A \to I^\bullet$ in Mod_G, $H^n(G, A) = H^n(\mathrm{Hom}_G(\mathbb{Z}, I^\bullet))$. And because $G' \to G$ is an isomorphism, $f^* : \mathrm{Mod}_G \to \mathrm{Mod}_{G'}$ is an catagory equivalence. So $f^*A \to f^*I^\bullet$ is an injective resolution in $\mathrm{Mod}_{G'}$. Thus σ_t comes from the following diagram of complexes:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}, I^0) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}, I^1) & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \text{“id”}} & & \downarrow{\scriptstyle \text{“id”}} & & \\
0 & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}, I^0) & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}, I^1) & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle u^*} & & \downarrow{\scriptstyle u^*} & & \\
0 & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}, I^0) & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}, I^1) & \longrightarrow & \ldots
\end{array}$$

It suffices to show that the middle vertical map u^* is the identity.

Recall that $\mathrm{Hom}_G(\mathbb{Z}, A) \simeq A^G$. u^* is given by left multiplication by t. So easily we have $u^* = \mathrm{id}$. So σ_t is the identity map. □

Homework 10.3. Show that $H^1(G, A)$ is in bijection with isomorphism classes of G-torsors over A.

Proof. First construct the map:

$$\alpha : \{\text{isomorphism classes of } G\text{-torsors over } A\} \to H^1(G, A)$$

For $[X]$ an isomorphism class of G-torsors over A, we choose a basis point $x_0 \in X$. Because the action of A on X is freely transitive, there exists a unique $c(g) \in A$ such that

$$gx_0 = x_0 + c(g)$$

Hence we get a map $c : G \to A$.

Claim: c is a 1-cocycle. For $g_1, g_2 \in G$,

$$\begin{aligned} g_1g_2x_0 &= g_1(x_0 + c(g_2)) \\ &= g_1x_0 + g_1c(g_2) \\ &= x_0 + c(g_1) + g_1c(g_2) \end{aligned}$$

Claim: The cohomology class $[c]$ does not depend on the choice of basis point x_0. If we choose another basis point $x_1 = x_0 + a$ for some $a \in A$, then the corresponding cocycle c' satisfies:

$$\begin{aligned} gx_1 &= g(x_0 + a) \\ &= gx_0 + ga \\ &= x_0 + c(g) + ga \\ &= x_1 + c(g) + ga - a \end{aligned}$$

So $c'(g) = c(g) + ga - a$. So $[c'] = [c]$ in $H^1(G, A)$.

Define $\alpha([X]) = [c]$.

Claim: The map α is injective. For $[X_1], [X_2]$ two isomorphism classes of G-torsors over A, suppose $\alpha([X_1]) = \alpha([X_2])$. Choose basis points $x_1 \in X_1, x_2 \in X_2$. Let c_1, c_2 be the corresponding cocycles. So there exists $a \in A$ such that:

$$c_1(g) - c_2(g) = ga - a$$

We now construct an isomorphism of G-torsors $\phi : X_1 \to X_2$ by defining $\phi(x_1+b) = x_2+b+a$

for all $b \in A$. It is set-theoretically bijective. We check that it is G-equivariant:

$$\begin{aligned}\phi(g(x_1 + b)) &= \phi(gx_1 + gb) \\ &= \phi(x_1 + c_1(g) + gb) \\ &= x_2 + c_1(g) + gb + a \\ &= x_2 + c_2(g) + gb + a + ga - a \\ &= gx_2 + gb + ga \\ &= g(x_2 + b + a) \\ &= g\phi(x_1 + b)\end{aligned}$$

So ϕ is an isomorphism of G-torsors. Thus $[X_1] = [X_2]$, hence α is injective.

Claim: The map α is surjective. For $[c] \in H^1(G, A)$ represented by a cocycle $c : G \to A$, we construct a G-torsor X over A as follows: X is the set A with G-action defined by:

$$g * a := ga + c(g)$$

We check that X is a G-torsor over A:

- The action of A on X is given by addition, which is freely transitive.
- The action of A on X is compatible with the G-action:

$$\begin{aligned}g * (a + a') &= ga + a' + c(g) \\ &= (g * a) + (ga')\end{aligned}$$

- The G-action is well-defined:

$$\begin{aligned}g_1 * (g_2 * a) &= g_1 * (g_2 a + c(g_2)) \\ &= g_1 g_2 a + c(g_2) + c(g_1) \\ &= g_1 g_2 a + c(g_1 g_2) \quad \text{(by cocycle condition)} \\ &= (g_1 g_2) * a\end{aligned}$$

By construction, $\alpha([X]) = [c]$. Thus α is surjective. □

11 2025.11.20

11.1 Results on homology

Let $H \leq G$.

- **Shapiro's Lemma:** $H_i(G, \mathrm{ind}_H^G A) \cong H_i(H, A)$.
- Let $f : G' \to G$ be a group homomorphism. For $A \in \mathrm{Mod}_G$, we have $f^*A \in \mathrm{Mod}_{G'}$. This induces a map:
$$H_i(G', f^*A) \longrightarrow H_i(G, A)$$
- **Corestriction:** $\mathrm{Cor} : H_i(H, A) \longrightarrow H_i(G, A)$.
- **Coinflation:** $\mathrm{coinf} : H_i(G, A) \longrightarrow H_i(G/H, A_H)$ (where $H \trianglelefteq G$).

Assume $[G : H] < \infty$. We have the **Restriction** map $\mathrm{Res} : H_i(G, A) \to H_i(H, A)$. (Note: This comes from

$$H_i(G, A) \to H_i(G, \mathrm{Ind}_H^G \mathrm{Res}_H^G A) \xrightarrow{\cong} H_i(H, \mathrm{ind}_H^G \mathrm{Res}_H^G A) \xrightarrow{\cong} H_i(H, A)$$

the first isomorphism is because $[G : H] < \infty$ and the second isomorphism is because of Shapiro's Lemma)

Remark: The restriction map on H_0 is given by the Norm map $N_{G/H}$:

$$\begin{aligned} \mathrm{Res} : H_0(G, A) &\longrightarrow H_0(H, A) \\ A_G &\longrightarrow A_H \\ [a] &\longmapsto \left[\sum_{g \in H \backslash G} ga \right] \end{aligned}$$

where the sum runs over a set of right coset representatives.

Proposition 11.1.

(1) $H_i(G, A) = 0$ for all $i > 0$ for any relatively projective module A.

(2) If $[G : H] = m$, then $\mathrm{Cor} \circ \mathrm{Res}$ is the multiplication by m.

Corollary 11.1. If $|G| = m$, then:

1. $H_i(G, A)$ is m-torsion for all $i > 0$.

2. If A is a G-module of finite type, then $H_i(G, A)$ is finite.

Proposition 11.2. $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$.

Exercise 11.1. Verify Res : $H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Z})$ coincides with the transfer map Ver : $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ we defined before.

Proof of proposition. Consider the exact sequence

$$\begin{aligned} 0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] &\longrightarrow \mathbb{Z} \longrightarrow 0 \\ \sum a_g g &\longmapsto \sum a_g \end{aligned}$$

From $H_0(G, A) \cong A/I_G A$, this gives the long exact sequence in homology:

$$\underbrace{H_1(G, \mathbb{Z}[G])}_{0} \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow H_0(G, I_G) = I_G/I_G^2 \xrightarrow{\alpha} H_0(G, \mathbb{Z}[G]) \cong \mathbb{Z}[G]/I_G$$

α is artually zero homomorphism, so we have $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$.

Want to show $G^{\mathrm{ab}} \cong I_G/I_G^2$.

Define $\alpha : G \to I_G/I_G^2$. Recall I_G is the free $\mathbb{Z}$-module generated by $g - 1$ for all $g \in G$.

$$g \longmapsto \overline{g-1}$$

Claim: α is a group homomorphism.

$$\begin{aligned} \alpha(g_1 g_2) &= \overline{g_1 g_2 - 1} \\ &= \overline{(g_1 - 1)(g_2 - 1) + (g_1 - 1) + (g_2 - 1)} \\ &= \alpha(g_1) + \alpha(g_2) \quad (\text{since } (g_1 - 1)(g_2 - 1) \in I_G^2) \end{aligned}$$

Therefore, $G \xrightarrow{\alpha} I_G/I_G^2$ factors through G^{ab}.

Define $\beta : I_G \to G^{\mathrm{ab}}$ by $g - 1 \mapsto [g]$. We can check it's a group homomorphism, and it factors through I_G/I_G^2. Moreover, α and β are inverse to each other. □

V. Tate cohomology and Tate-Nakayama Theorem

11.2 Definition

From now on, let G always be a finite group.

Goal: Given a short exact sequence $0 \to A \to B \to C \to 0$, we have exact sequences:

$$0 \longrightarrow H^0(G,A) \longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \longrightarrow H^1(G,A) \longrightarrow \dots$$

and

$$\cdots \longrightarrow H_1(G,C) \longrightarrow H_0(G,A) \longrightarrow H_0(G,B) \longrightarrow H_0(G,C) \longrightarrow 0$$

We want to combine $H_i(G,-)$ and $H^i(G,-) \rightsquigarrow$ Tate cohomology $\hat{H}^i(G,-)$, $i \in \mathbb{Z}$.

Define **the norm map** $N^* : H_0(G,A) \to H^0(G,A)$. Consider the map $N : A \to A$ defined by $a \mapsto N(a) := \sum_{g\in G} ga$. We have the following diagram:

$$\begin{array}{ccc} A_G & \xrightarrow{N^*} & A^G \\ \uparrow\!\uparrow & & \downarrow\!\downarrow \\ A & \xrightarrow{N} & A \end{array}$$

Easily check that $\mathrm{Im}(N) \subseteq A^G$. For any $g \in G$,

$$N((g-1)a) = \sum_{g'\in G} g'(g-1)a = 0.$$

Thus, $I_G A \subseteq \mathrm{Ker}(N)$, so the map factors through A_G. So we get the norm map $N^* : A_G \to A^G$ from N.

Definition 11.1. The **Tate cohomology groups** are defined as follows:

$$\begin{aligned} \hat{H}^n(G,A) &= H^n(G,A) \quad \forall n \geq 1 \\ \hat{H}^{-n}(G,A) &= H_{n-1}(G,A) \quad \forall n \geq 2 \\ \hat{H}^{-1}(G,A) &= \ker N^* = \frac{\ker N}{I_G A} \\ \hat{H}^0(G,A) &= \mathrm{coker} N^* = \frac{A^G}{NA} \end{aligned}$$

Example 11.1.

$$\begin{aligned} \hat{H}^0(G,\mathbb{Z}) &= \mathrm{coker}\left(\mathbb{Z} \xrightarrow{\cdot|G|} \mathbb{Z}\right) = \mathbb{Z}/|G|\mathbb{Z} \\ \hat{H}^{-1}(G,\mathbb{Z}) &= \ker\left(\mathbb{Z} \xrightarrow{\cdot|G|} \mathbb{Z}\right) = 0 \end{aligned}$$

Theorem 11.1. Let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. Then we have the long exact sequence:

$$\begin{aligned}\cdots \longrightarrow \hat{H}^{-2}(G,C) &\longrightarrow \hat{H}^{-1}(G,A) \longrightarrow \hat{H}^{-1}(G,B) \longrightarrow \hat{H}^{-1}(G,C)\\ &\longrightarrow \hat{H}^{0}(G,A) \longrightarrow \hat{H}^{0}(G,B) \longrightarrow \hat{H}^{0}(G,C)\\ &\longrightarrow \hat{H}^{1}(G,A) \longrightarrow \dots\end{aligned}$$

Moreover, if A is relatively injective (=relatively projective), we have $\hat{H}^n(G,A) = 0$ for all $n \in \mathbb{Z}$.

Proof. The first statement comes from the Snake lemma.

$$\begin{array}{ccccccccc}
 & & \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & \longrightarrow & \hat{H}^0(G,C) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow & H^1(G,A) \to \dots \\
 & & \uparrow{\scriptstyle N^*} & & \uparrow{\scriptstyle N^*} & & \uparrow{\scriptstyle N^*} & & \\
\cdots \to H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \hat{H}^{-1}(G,A) & \longrightarrow & \hat{H}^{-1}(G,B) & \longrightarrow & \hat{H}^{-1}(G,C) & &
\end{array}$$

For the second statement, $\hat{H}^i(G,A) = 0$ for all $i \in (-\infty,-2] \cup [1,+\infty)$. Want to show $\hat{H}^{-1}(G,A) = 0 = \hat{H}^0(G,A)$.

We may assume $A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ where X is an abelian group. Consider the map $N^* : A_G \to A^G$. We have $A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X) \cong X$, $A^G = \{(\sum_{g\in G} g) \otimes x \mid x \in X\} \cong X$.

And the map N^* corresponds to the id_X (induced by $1 \otimes x \mapsto \sum g \otimes x$, but under the identification $A_G \cong X$ and $A^G \cong X$, it behaves as identity). So N^* is an isomorphism, then $\hat{H}^0(G,A) = \hat{H}^{-1}(G,A) = 0$. □

Corollary 11.2 (**Dimension shifting**)**.** Let $0 \to A \to I \to B \to 0$ be an exact sequence with I relatively injective. Then $\hat{H}^n(G,B) \cong \hat{H}^{n+1}(G,A)$ for all $n \in \mathbb{Z}$.

Definition 11.2. Restriction: $\mathrm{Res} : \hat{H}^n(G,-) \to \hat{H}^n(H,-)$ (where $H \le G$). Already done for $n \ge 1$ and $n \le -2$. We now define it for $n = 0, -1$.

For $n = 0$:

$$\begin{array}{ccc} H^0(G,A) = A^G & \xrightarrow{\text{Res}} & H^0(H,A) = A^H \\ \downarrow & & \downarrow \\ \hat{H}^0(G,A) = A^G/N_G A & \xrightarrow{\text{Res}} & \hat{H}^0(H,A) = A^H/N_H A \end{array}$$

Note that $N_G(A) \subseteq N_H(A)$.

For $n = -1$:

$$\begin{array}{ccc} H_0(G,A) = A_G & \xrightarrow{\text{Res}} & H_0(H,A) = A_H \\ \uparrow & & \uparrow \\ \hat{H}^{-1}(G,A) = \frac{\ker N_G}{I_G A} & \xrightarrow{\text{Res}} & \hat{H}^{-1}(H,A) = \frac{\ker N_H}{I_H A} \end{array}$$

$$\begin{array}{ccc} H_0(G,A) = A_G & \xrightarrow{\text{Res}=N_{G/H}} & H_0(H,A) = A_H \\ [a] & \longmapsto & [N'_{G/H}(a)] \end{array}$$

Here $N'_{G/H}(a) = \sum_{\bar{g} \in H\backslash G} ga$. It suffices to check $N'_{G/H}(\ker N_G) \subseteq \ker N_H$. For all $a \in \ker N_G$, $N_H(N'_{G/H}(a)) = N_G(a) = 0$.

Lemma 11.1. The restriction map $\text{Res} : \hat{H}^n(G,-) \longrightarrow \hat{H}^n(H,-)$ is compatible with exact sequences.

Proof Sketch. It suffices to show the diagram is commutative for any $0 \to A \to B \to C \to 0$.

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

This can be done by direct computation. □

Exercise 11.2. Define $\text{Cor} : \hat{H}^n(H,-) \longrightarrow \hat{H}^n(G,-)$ and check that it's compatible with exact sequence.

Corollary 11.3.

1. Cor $\circ$ Res is multiplication by $[G:H]$ in $\hat{H}^n(G,A)$.
2. The group $\hat{H}^n(G,A)$ is killed by $|G|$ for all $n \in \mathbb{Z}$.
3. If A is a G-module of finite type, then $\hat{H}^n(G,A)$ are finite for all $n \in \mathbb{Z}$.

Proof. By dimension shift. □

11.3 Cup product

If P is left G-module it can also be viewed as a right G-module by:

$$a \cdot g := g^{-1}a$$

Definition 11.3. $P^* = \mathrm{Hom}_{\mathbb{Z}}(\underbrace{P}_{\text{right } \mathbb{Z}[G]\text{-module}}, \mathbb{Z})$. It is a left G-module.

Example 11.2. $P = \mathbb{Z}[G]$. You can check that: $\mathbb{Z}[G] \xrightarrow{\simeq} \mathbb{Z}[G]^* : g \to (g^* : h \mapsto \delta_{g,h})$ is a left G-module isomorphism.

Let $\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$ be a resolution of $\mathbb{Z}$ by finite free $\mathbb{Z}[G]$-modules (e.g. Standard resolution).

Take $(-)^* = \mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{Z})$:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varepsilon^*} \underbrace{P_0^*}_{P_{-1}} \longrightarrow \underbrace{P_1^*}_{P_{-2}} \longrightarrow \underbrace{P_2^*}_{P_{-3}} \cdots$$

Definition 11.4. Define $P_n := P^*_{-n-1}$ for all $n \leq -1$. These are finite free $\mathbb{Z}[G]$-modules. The sequence

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\partial} P_{-1} \longrightarrow P_{-2} \longrightarrow P_{-3} \longrightarrow \cdots$$

constructed by splicing $P_0 \xrightarrow{\varepsilon} \mathbb{Z} \xrightarrow{\varepsilon^*} P_0^*$ (i.e., $\partial = \varepsilon^* \circ \varepsilon$) is exact. It is called a **complete resolution** of $\mathbb{Z}$.

Proposition 11.3. $\hat{H}^n(G,A) = H^n(\mathrm{Hom}_G(P_\bullet, A))$.

Proof. $n \geq 1$. OK!

$n \leq -2$. Recall $A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$.

$$\mathrm{Hom}_G(P_n, A) = \mathrm{Hom}_G(P^*_{-n-1}, A) \cong P_{-n-1} \otimes_{\mathbb{Z}[G]} A \quad \text{as abelian groups.}$$

(Note: P_{-n-1} is free $\mathbb{Z}[G]$-module. Consider the case $P = \mathbb{Z}[G]$, using $\mathbb{Z}[G]^* \cong \mathbb{Z}[G]$ to see the isomorphism).

$n = -1, 0$, there is a **fact**: The following diagram commutes:

$$\begin{array}{ccc} P_0 \otimes_{\mathbb{Z}[G]} A & \xrightarrow{\simeq} & \mathrm{Hom}_G(P_{-1}, A) \\ \downarrow{\scriptstyle \varepsilon \otimes \mathrm{id}} & & \downarrow{\scriptstyle \epsilon^* \circ -} \\ \mathbb{Z} \otimes_{\mathbb{Z}[G]} A = A_G & \xrightarrow{N_G} & \mathrm{Hom}_G(\mathbb{Z}, A) = A^G \end{array}$$

Use the two exact sequence:

$$P_1 \otimes_{\mathbb{Z}[G]} A \longrightarrow P_0 \otimes_{\mathbb{Z}[G]} A \xrightarrow{\varepsilon \otimes \mathrm{id}} A_G \longrightarrow 0$$

$$0 \longrightarrow A^G \xrightarrow{\varepsilon^* \circ -} \mathrm{Hom}_G(P_0, A) \longrightarrow \mathrm{Hom}_G(P_1, A)$$

and natural diagram:

$$\begin{array}{ccc} P_1 \otimes_{\mathbb{Z}[G]} A & \xrightarrow{\simeq} & \mathrm{Hom}_G(P_{-2}, A) \\ \downarrow{\scriptstyle (P_1 \to P_0) \otimes \mathrm{id}} & & \downarrow{\scriptstyle (P_0^* \to P_1^*) \circ -} \\ P_0 \otimes_{\mathbb{Z}[G]} A & \xrightarrow{\simeq} & \mathrm{Hom}_G(P_{-1}, A) \end{array}$$

We have:

$$\begin{aligned} \ker(N_G) &\cong \frac{\ker(P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \to A^G)}{\ker(P_0 \otimes_{\mathbb{Z}[G]} A \to A_G)} \\ &= \frac{\ker(P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \to A^G \to \mathrm{Hom}_G(P_0, A))}{\mathrm{Im}(P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A)} \\ &\cong \frac{\ker(\mathrm{Hom}_G(P_{-1}, A) \to \mathrm{Hom}_G(P_0, A))}{\mathrm{Im}(\mathrm{Hom}_G(P_{-2}, A) \to \mathrm{Hom}_G(P_{-1}, A))} \\ &= H^{-1}(\mathrm{Hom}_G(P_\bullet, A)) \end{aligned}$$

Similarly,

$$\begin{aligned}
\operatorname{coker}(N_G) &= \frac{A^G}{\operatorname{Im}(A_G \to A^G)} \\
&\cong \frac{\operatorname{Im}(A^G \to \operatorname{Hom}_G(P_0, A))}{\operatorname{Im}(A_G \to A^G \to \operatorname{Hom}_G(P_0, A))} \\
&\cong \frac{\ker(\operatorname{Hom}_G(P_0, A) \to \operatorname{Hom}_G(P_1, A))}{\operatorname{Im}(P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \to A^G \to \operatorname{Hom}_G(P_0, A))} \\
&= \frac{\ker(\operatorname{Hom}_G(P_0, A) \to \operatorname{Hom}_G(P_1, A))}{\operatorname{Im}(\operatorname{Hom}_G(P_{-1}, A) \to \operatorname{Hom}_G(P_0, A))} \\
&= H^0(\operatorname{Hom}_G(P_\bullet, A))
\end{aligned}$$

□

Theorem 11.2. There exists a unique family of bilinear maps

$$\hat{H}^p(G, A) \times \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, C)$$

for any $p, q \in \mathbb{Z}$ and any pairing $A \times B \to C$ of G-modules, satisfying:

1. For $p = q = 0$, these maps are induced by natural map $A^G \times B^G \to C^G$.
2. They are functorial.
3. 3.1 Let B be a G-module. Let $0 \to A' \to A \to A'' \to 0$ and $0 \to C' \to C \to C'' \to 0$ be exact sequences of G-modules. We assume that we have a pairing $A \times B \to C$ which induces pairings $A' \times B \to C'$ and $A'' \times B \to C''$. Then $\forall \alpha'' \in \hat{H}^p(G, A'')$, $\beta \in \hat{H}^q(G, B)$, we have:

$$\delta\alpha'' \cup \beta = \delta(\alpha'' \cup \beta) \in \hat{H}^{p+q+1}(G, C')$$

where $\delta : \hat{H}^p(G, A'') \to \hat{H}^{p+1}(G, A')$.

3.2 Let $0 \to B' \to B \to B'' \to 0$ and $0 \to C' \to C \to C'' \to 0$ be exact sequences of G-modules. $A \in \mathrm{Mod}_G$. Assume that we have a pairing $A \times B \to C$ which induces pairing $A \times B' \to C'$ and $A \times B'' \to C''$. Then $\forall \alpha \in \hat{H}^p(G, A)$, $\forall \beta'' \in \hat{H}^q(G, B'')$, we have

$$\alpha \cup \delta\beta'' = (-1)^p \delta(\alpha \cup \beta'') \in \hat{H}^{p+q+1}(G, C').$$

Remark: The pairing $f : A \times B \to C$ of G-modules needs:

$$f(ga, gb) = gf(a, b)$$

This will give $A \otimes_{\mathbb{Z}} B \to C$ and the G-module structure on $A \times_{\mathbb{Z}} B$ is:

$$ga \otimes b = (ga) \otimes (gb)$$

Lemma 11.2. Let $(P_\bullet, d)$ be the complete standard resolution of $\mathbb{Z}$. Then there exists a family of homomorphisms $\varphi_{p,q} : P_{p+q} \to P_p \otimes P_q$ for all $p, q \in \mathbb{Z}$ satisfying:

1. $\varphi_{p,q} \circ d = (d \otimes 1)\varphi_{p+1,q} + (-1)^p(1 \otimes d)\varphi_{p,q+1}$.
2. $(\varepsilon \otimes \varepsilon)\varphi_{0,0} = \varepsilon$, where $\varepsilon : P_0 = \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z}, g \mapsto 1$.

Remark: Lemma implies that there is a homomorphism of chain complexes $\varphi : P_\bullet \to \mathrm{Tot}(P_\bullet \otimes P_\bullet)$.

Construction of $\varphi_{p,q}$:

$$\begin{aligned} &n \geq 0, \quad P_n = \mathbb{Z}[G^{n+1}] \\ &n \geq 1, \quad P_{-n} = P^*_{-1+n} \cong \mathbb{Z}[G^n] \end{aligned}$$

$$\begin{aligned} &p, q \geq 0. \quad \varphi_{p,q}(g_0, \ldots, g_{p+q}) = (g_0, \ldots, g_p) \otimes (g_p, \ldots, g_{p+q}) \\ &p, q \geq 1. \quad \varphi_{-p,-q}(g_1, \ldots, g_{p+q})^* = (g_1, \ldots, g_p)^* \otimes (g_{p+1}, \ldots, g_{p+q})^* \end{aligned}$$

For $p \geq 0$ and $q \geq 1$:

$$\begin{aligned} \varphi_{p,-p-q}(g_1, \ldots, g_q)^* &= \sum_{(h_1,\ldots,h_p)\in G^p} (g_1, h_1, \ldots, h_p) \otimes (h_p, \ldots, h_1, g_1, \ldots, g_q)^* \\ \varphi_{-p-q,p}(g_1, \ldots, g_q)^* &= \sum_{(h_1,\ldots,h_p)\in G^p} (g_1, \ldots, g_q, h_1, \ldots, h_p)^* \otimes (h_p, \ldots, h_1, g_q) \\ \varphi_{p+q,-q}(g_0, \ldots, g_p) &= \sum_{(h_1,\ldots,h_q)\in G^q} (g_0, \ldots, g_p, h_1, \ldots, h_q) \otimes (h_q, \ldots, h_1)^* \\ \varphi_{-q,p+q}(g_0, \ldots, g_p) &= \sum_{(h_1,\ldots,h_q)\in G^q} (h_1, \ldots, h_q)^* \otimes (h_q, \ldots, h_1, g_0, \ldots, g_p) \end{aligned}$$

Proof of Theorem (1). $A \times B \longrightarrow C$ factors through $A \otimes_{\mathbb{Z}} B$. It suffices to show $\cup$ for $C = A \otimes_{\mathbb{Z}} B$.

Define: $f \in \mathrm{Hom}_G(P_p, A)$, $g \in \mathrm{Hom}_G(P_q, B)$.

$$f \cup g := (f \otimes g) \circ \varphi_{p,q}$$

$$P_{p+q} \xrightarrow{\varphi_{p,q}} P_p \otimes P_q \xrightarrow{f\otimes g} A \otimes B$$

$$\begin{aligned} d(f \cup g) &= (f \otimes g) \circ \varphi_{p,q} \circ d \\ &= (f \otimes g) \circ ((d \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes d) \circ \varphi_{p,q+1}) \\ &= df \cup g + (-1)^p f \cup dg \end{aligned}$$

If f and g are cocycles $\implies$ $f \cup g$ is a cocycle.
If f cocycle, g coboundary, $g = d\tilde{g}$, we need to prove $f \cup g$ is a coboundary.
Claim: $f \cup g = d(f \cup \tilde{g}) \cdot (-1)^p$.

$$d(f \cup \tilde{g}) = df \cup \tilde{g} + (-1)^p f \cup d\tilde{g} = (-1)^p f \cup g.$$

Similarly f coboundary, g cocycle. Then $f \cup g = d(\tilde{f} \cup g)$. Hence $\cup$ is defined for cohomology.

$$\cup : \hat{H}^p(G, A) \times \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes B) \longrightarrow \hat{H}^{p+q}(G, C).$$

When $p = q = 0$,

$$\begin{array}{ccc} \mathrm{Hom}_G(\mathbb{Z}[G], A) \times \mathrm{Hom}_G(\mathbb{Z}[G], B) & \xrightarrow{\quad\cup\quad} & \mathrm{Hom}_G(\mathbb{Z}[G], C) \\ \uparrow{\scriptstyle j_\varepsilon} & & \uparrow{\scriptstyle j_\varepsilon} \\ A^G \times B^G = \mathrm{Hom}_G(\mathbb{Z}, A) \times \mathrm{Hom}_G(\mathbb{Z}, B) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}, C) = C^G \end{array}$$

□

Proof of (3.1). Recall: $\hat{H}^n(G, A) = H^n(\mathrm{Hom}_G(P_\bullet, A))$ where $P_\bullet$ is a complete standard resolution of $\mathbb{Z}$. $C^n(A) = \mathrm{Hom}_G(P_n, A) \supseteq Z^n(A) \supseteq B^n(A)$ where $Z^n(A) = \ker d$ (cocycles) and $B^n(A) = \mathrm{im} d$ (coboundaries).

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

P_n is free $\mathbb{Z}[G]$-module $\implies$ $\mathrm{Hom}_G(P_n, -)$ is exact. We have the following commutative

diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & C^n(A')/B^n(A') & \longrightarrow & C^n(A)/B^n(A) & \longrightarrow & C^n(A'')/B^n(A'') & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & C^n(A') & \longrightarrow & C^n(A) & \longrightarrow & C^n(A'') & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle d} & & \uparrow{\scriptstyle d} & & \uparrow{\scriptstyle d} & & \\
0 & \longrightarrow & C^{n-1}(A') & \longrightarrow & C^{n-1}(A) & \longrightarrow & C^{n-1}(A'') & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & Z^{n+1}(A') & \longrightarrow & Z^{n+1}(A) & \longrightarrow & Z^{n+1}(A'') & &
\end{array}$$

And then consider:

$$\begin{array}{ccccccccc}
 & & \hat{H}^n(G,A') & & \hat{H}^n(G,A) & & \hat{H}^n(G,A'') & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & C^n(A')/B^n(A') & \longrightarrow & C^n(A)/B^n(A) & \longrightarrow & C^n(A'')/B^n(A'') & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\
0 & \longrightarrow & Z^{n+1}(A') & \longrightarrow & Z^{n+1}(A) & \longrightarrow & Z^{n+1}(A'') & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \hat{H}^{n+1}(G,A') & & \hat{H}^{n+1}(G,A) & & \hat{H}^{n+1}(G,A'') & &
\end{array}$$

We can describe the connecting homomorphism $\delta : \hat{H}^p(G, A'') \to \hat{H}^{p+1}(G, A')$ as follows: Let $a'' \in Z^p(A'')$ be a cocycle for α''. Let $a \in C^p(A)$ be a lifting for a''. Then $\delta\alpha'' = [da]$.

Similarly $\delta(\alpha'' \cup \beta) = [d(a \cup b)]$ for $b \in Z^q(B)$, $[b] = \beta$. Want to show $\delta\alpha'' \cup \beta = \delta(\alpha'' \cup \beta)$.

$$\text{LHS} = [da \cup b] \quad \text{RHS} = [d(a \cup b)]$$

It suffices to show $da \cup b = d(a \cup b)$. It is easy:

$$d(a \cup b) = da \cup b + (-1)^p a \cup \underbrace{db}_{0 \text{ as } b \in Z^q(B)}$$

□

11.4 Homework

Homework 11.1. Show that Res : $H_1(G,\mathbb{Z}) \to H_1(H,\mathbb{Z})$ coincide with the transfer map Ver : $G^{ab} \to H^{ab}$ that we defined before.

Proof.

$$\begin{array}{ccccccc} G^{ab} & \xrightarrow{\simeq} & I_G/I_G^2 & \xrightarrow{\simeq} & H_1(G;\mathbb{Z}) & \xrightarrow{\simeq} & H_0(G;I_G) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \text{Res}} \\ H^{ab} & \xrightarrow{\simeq} & I_H/I_H^2 & \xrightarrow{\simeq} & H_1(H;\mathbb{Z}) & \xrightarrow{\simeq} & H_0(H;I_H) \end{array}$$

$\{x_1,\dots,x_m\}$ is the representative set of right cosets of H in G.

$$\begin{aligned} \text{Res}([g-1]) &= \left[\sum_{j=1}^{m} x_j(g-1)\right] = \left[\sum_{j=1}^{m}(h_j x_{\sigma(j)} - x_j)\right] \\ &= \left[\sum_{j=1}^{m}(h_j-1)(x_{\sigma(j)}-1) + \sum_{j=1}^{m}(h_j-1)\right] \\ &= \sum_{j=1}^{m}[(h_j-1)] \end{aligned}$$

So the map $G^{ab} \to H^{ab}$ sends $[g]$ to $[h_1 \dots h_m]$. □

Homework 11.2. Define the corestriction Cor : $\hat{H}^n(H,-) \to \hat{H}^n(G,-)$ and check that Cor and Res are both compatible with exact sequences.

The Definition of Cor.

1. When $n \leqslant -2$, we have given

$$\text{Cor} : \hat{H}^n(H;A) = H_{-n-1}(H;A) \to \hat{H}^n(G;A) = H_{-n-1}(G;A)$$

2. When $n \geqslant 1$, we have given

$$\text{Cor} : \hat{H}^n(H;A) = H^n(H;A) \to \hat{H}^n(G;A) = H^n(G;A)$$

3. When $n = -1$, we have given Cor : $H_0(H;A) \to H_0(G;A)$, $\hat{H}^{-1}(*)$ can be considered as a subset of $H^0(*)$. So we can define:

$$\text{Cor} := \text{Cor}|_{\hat{H}^{-1}(H;A)} : \hat{H}^{-1}(H;A) \to \hat{H}^{-1}(G;A)$$

4. When $n = 0$, we have given $\mathrm{Cor} : H^0(H;A) \to \hat{H}^0(G;A) = H^0(G;A)$, $\hat{H}^0(*)$ can be considered as a quotient of $H^0(*)$. So we can define:

$$\mathrm{Cor} := \mathrm{Cor}/\sim : \hat{H}^0(H;A) \to \hat{H}^0(G;A)$$

□

Proof of compatibility of Cor. It suffices to show the following diagram commutes for any G-module short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$:

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

$$\begin{array}{ccccccccc} & & & & \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & \longrightarrow & \hat{H}^0(G,C) \\ & & & & \uparrow\uparrow & & \uparrow\uparrow & & \uparrow\uparrow \\ & & 0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) \longrightarrow H^1(G,A) \to \dots \\ & & & & \uparrow{\scriptstyle N^*} & & \uparrow{\scriptstyle N^*} & & \uparrow{\scriptstyle N^*} \\ \cdots \to H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ & & \hat{H}^{-1}(G,A) & \longrightarrow & \hat{H}^{-1}(G,B) & \longrightarrow & \hat{H}^{-1}(G,C) & & \end{array}$$

For $[c] \in \hat{H}^{-1}(H;C) \subseteq H_0(H;C) = C_H = C/I_H C$, $c \in C$, $[a] := \delta(c) \in \hat{H}^0(H;A) = \frac{H^0(H;A)}{*} = \frac{A^H}{*}$ for $a \in A^H$ is given by: $g(b) = c$ for some $b \in B$, $f(a) = N_H^*[b]$.

For $\mathrm{Cor}[c] = [c] \in \hat{H}^{-1}(G;C)$, we can get $[a'] \in \hat{H}^0(G;A)$ in the same way. Our goal is to show that:

$$\mathrm{Cor}[a] = \left[\sum_{g \in G/H} ga\right] = [a']$$

It is because the following equivalence:

$$f\left(\sum_{g\in G/H} ga\right) = \sum_{g\in G/H} gf(a) = \sum_{g\in G/H} gN_H^*[b] = \sum_{g\in G/H} g\sum_{h\in H} hb = \sum_{g\in G} gb = N_G^*[b]$$

□

Homework 11.3. Extend Shapiro's Lemma to Tate Cohomology $\hat{H}^n$ for all $n \in \mathbb{Z}$.

Proof. We prove the isomorphism $\hat{H}^n(G, \mathrm{Ind}_H^G A) \cong \hat{H}^n(H, A)$ for all $n \in \mathbb{Z}$ by separating cases.

Case 1: $n \geq 1$**.**

For positive degrees, Tate cohomology coincides with ordinary cohomology: $\hat{H}^n \cong H^n$. By the standard cohomological Shapiro's Lemma:

$$\hat{H}^n(G, \mathrm{Ind}_H^G A) = H^n(G, \mathrm{Ind}_H^G A) \cong H^n(H, A) = \hat{H}^n(H, A)$$

Case 2: $n \leq -2$**.**

For these degrees, Tate cohomology corresponds to ordinary homology with a shift in index: $\hat{H}^n(G, -) \cong H_{-(n+1)}(G, -)$. Because G is finite, induction and coinduction coincide. By the standard homological Shapiro's Lemma:

$$\hat{H}^n(G, \mathrm{Ind}_H^G A) = H_{-n-1}(G, \mathrm{Ind}_H^G A) = H_{-n-1}(G, \mathrm{ind}_H^G A) \cong H_{-n-1}(H, A) \cong \hat{H}^n(H, A).$$

Case 3: $n = -1, 0$**.**

$M := \mathrm{Ind}_H^G A = \mathrm{ind}_H^G A$.

We utilize the fundamental 4-term exact sequence relating $\hat{H}^{-1}$ and $\hat{H}^0$:

$$0 \longrightarrow \hat{H}^{-1}(G, X) \longrightarrow H_0(G, X) \xrightarrow{N_G} H^0(G, X) \longrightarrow \hat{H}^0(G, X) \longrightarrow 0$$

We construct a commutative diagram between the sequence for A (as H-module) and M (as G-module):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \hat{H}^{-1}(H, A) & \longrightarrow & H_0(H, A) & \xrightarrow{N_H} & H^0(H, A) & \longrightarrow & \hat{H}^0(H, A) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \cong\downarrow{\scriptstyle \beta} & & \cong\downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \\
0 & \longrightarrow & \hat{H}^{-1}(G, M) & \longrightarrow & H_0(G, M) & \xrightarrow{N_G} & H^0(G, M) & \longrightarrow & \hat{H}^0(G, M) & \longrightarrow & 0
\end{array}$$

Defining the vertical maps:

- $\beta : H_0(H, A) \xrightarrow{\sim} H_0(G, M)$ is the homological Shapiro isomorphism (In fact is trivial by $\mathbb{Z} \otimes_{\mathbb{Z}[H]} A \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$.)
- $\gamma : H^0(H, A) = A^H \xrightarrow{\sim} H^0(G, M) = M^G$ is the map $a \mapsto \sum_{g \in G/H} g \otimes a$. This is an isomorphism (explicit verification of invariants in induced module).

Commutativity of the middle square:
For $a \in A$, let $[a]_H$ be its class in $H_0(H, A)$.

- Path $\rightarrow\downarrow$: $N_H([a]_H) = N_H(a) \in A^H$. Then $\gamma(N_H(a)) = \sum_{g \in G/H} g \otimes N_H(a)$.
- Path $\downarrow\rightarrow$: $\beta([a]_H) = [1 \otimes a]_G \in H_0(G, M)$. Then $N_G(1 \otimes a) = \sum_{\sigma \in G} \sigma(1 \otimes a)$.

Decomposing $\sigma \in G$ as gh with $g \in G/H, h \in H$:

$$\sum_{\sigma \in G} \sigma \otimes a = \sum_{g \in G/H} g \otimes \left(\sum_{h \in H} ha \right) = \sum_{g \in G/H} g \otimes N_H(a).$$

Thus the square commutes.
Conclusion:
Since β and γ are isomorphisms, the Five Lemma (or simple diagram chasing) implies that the induced maps on the kernels (α) and cokernels (δ) are isomorphisms.

$$\hat{H}^{-1}(H, A) \cong \hat{H}^{-1}(G, M) \quad \text{and} \quad \hat{H}^0(H, A) \cong \hat{H}^0(G, M).$$

□

Homework 11.4. Let H be a subgroup of G. Let A be a G-module and B an H-submodule of A. For any $\sigma \in G$, we set ${}^{\sigma}H = \sigma H \sigma^{-1}$.

(a) Show that the homomorphisms

$$ {}^{\sigma}H \to H,\ h \mapsto \sigma^{-1} h \sigma; \quad B \to \sigma B,\ b \mapsto \sigma b$$

are compatible and induce isomorphisms

$$\sigma_* : \hat{H}^n(H, B) \to \hat{H}^n({}^{\sigma}H, \sigma B)$$

for all $n \geq 0$.

(b) Show that if C is a G-module, we have for all $\alpha \in \hat{H}^p(H, A)$, $\gamma \in \hat{H}^q(H, C)$, $\sigma \in G$, the formula

$$\sigma_*(\alpha \cup \gamma) = \sigma_*(\alpha) \cup \sigma_*(\gamma).$$

Proof of (a). Denote $\varphi : H \to {}^{\sigma}H$ $\psi : B \to \sigma B$. To prove compatibility, we need to show the equivalence:

$$\psi(hb) = \varphi(h)\psi(b) \quad \text{for all } b \in B,\ h \in H.$$

As elements in G, LHS $= \sigma hb$, RHS $= (\sigma h\sigma^{-1})\sigma b = \sigma hb$. The equality holds, proving compatibility. Also easy to see φ and ψ are isomorphisms and their inverse are also compatible. So σ_* are all isomorphisms. □

Proof of (b). Let $P_\bullet$ be a complete resolution of $\mathbb{Z}$ by finitely generated free G-modules (as defined in Definition 11.4). Since $[G : H] < \infty$, $P_\bullet$ is also a complete resolution for the subgroup H.

Recall the definition of the cup product for Tate cohomology: There exists a family of G-homomorphisms $\varphi_{p,q} : P_{p+q} \to P_p \otimes P_q$ (diagonal approximation). For cochains $f \in \mathrm{Hom}_H(P_p, A)$ and $g \in \mathrm{Hom}_H(P_q, C)$, their cup product $f \cup g \in \mathrm{Hom}_H(P_{p+q}, A \otimes C)$ is defined by:

$$f \cup g = (f \otimes g) \circ \varphi_{p,q}.$$

Explicitly, for $x \in P_{p+q}$, if we write $\varphi_{p,q}(x) = \sum_i y_i \otimes z_i$ (where $y_i \in P_p, z_i \in P_q$), then:

$$(f \cup g)(x) = \sum_i f(y_i) \otimes g(z_i).$$

Now we consider the isomorphism $\sigma_* : \hat{H}^n(H, M) \to \hat{H}^n({}^\sigma H, \sigma M)$. On the cochain level, for any G-module M and $\phi \in \mathrm{Hom}_H(P_n, M)$, the cochain $\sigma_*\phi \in \mathrm{Hom}_{{}^\sigma H}(P_n, \sigma M)$ is defined by:

$$(\sigma_*\phi)(x) = \sigma \cdot \phi(\sigma^{-1}x) \quad \text{for all } x \in P_n.$$

(Note: Since P_n is a G-module, $\sigma^{-1}x$ is well-defined).

We verify the formula $\sigma_*(f \cup g) = (\sigma_* f) \cup (\sigma_* g)$. Let $x \in P_{p+q}$. Since $\varphi_{p,q}$ is a G-homomorphism (it commutes with the G-action), we have:

$$\varphi_{p,q}(\sigma^{-1}x) = \sigma^{-1} \cdot \varphi_{p,q}(x) = \sum_i (\sigma^{-1}y_i) \otimes (\sigma^{-1}z_i).$$

LHS Computation:

$$\begin{aligned}(\sigma_*(f \cup g))(x) &= \sigma \cdot \left[(f \cup g)(\sigma^{-1}x)\right] \\ &= \sigma \cdot \left[\sum_i f(\sigma^{-1}y_i) \otimes g(\sigma^{-1}z_i)\right] \\ &= \sum_i \sigma \cdot (f(\sigma^{-1}y_i) \otimes g(\sigma^{-1}z_i))\end{aligned}$$

The G-action on the tensor product $A \otimes C$ is diagonal, i.e., $\sigma(a \otimes c) = \sigma a \otimes \sigma c$. Thus:

$$= \sum_i (\sigma \cdot f(\sigma^{-1} y_i)) \otimes (\sigma \cdot g(\sigma^{-1} z_i)).$$

RHS Computation: By definition of the cup product for the cochains $\sigma_* f$ and $\sigma_* g$:

$$\begin{aligned}((\sigma_* f) \cup (\sigma_* g))(x) &= ((\sigma_* f) \otimes (\sigma_* g))(\varphi_{p,q}(x)) \\ &= ((\sigma_* f) \otimes (\sigma_* g)) \left(\sum_i y_i \otimes z_i \right) \\ &= \sum_i (\sigma_* f)(y_i) \otimes (\sigma_* g)(z_i) \\ &= \sum_i (\sigma \cdot f(\sigma^{-1} y_i)) \otimes (\sigma \cdot g(\sigma^{-1} z_i)).\end{aligned}$$

Comparing the LHS and RHS, we see they are identical on the cochain level. Thus, the induced cohomology classes satisfy:

$$\sigma_*(\alpha \cup \gamma) = \sigma_*(\alpha) \cup \sigma_*(\gamma).$$

□

Homework 11.5. Let G be a finite abelian group. Let A be an abelian group with trivial G-action. Let $s \in G = \hat{H}^{-2}(G, \mathbb{Z})$, let $f \in \mathrm{Hom}(G, A) = \hat{H}^1(G, A)$. Show that $s \cup f = f(s) \in \hat{H}^{-1}(G, A)$.

Recall **Example 10.1**: the isomorphism $H^1(G; A) \cong \mathrm{Hom}(G, A)$ holds when A is a trivial G-module.

Proof. Because we have **split** short exact sequence:

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

We have the exact sequence:

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

(Remark: The G-module structure of the elements in the sequence is as usual.)

Since $\mathbb{Z}[G] \otimes A$ is an induced module, its Tate cohomology vanishes. Thus, the connecting

homomorphism is an isomorphism:

$$\delta : \hat{H}^{-1}(G, A) \xrightarrow{\sim} \hat{H}^0(G, I_G \otimes A).$$

It suffices to show that the images of $f(s)$ and $s \cup f$ under d coincide in $\hat{H}^0(G, I_G \otimes A)$.

1. Image of $f(s)$: The element $f(s) \in A$ defines a class in $\hat{H}^{-1}(G, A)$. Following the description of δ (lifting to $\mathbb{Z}[G] \otimes A$ and taking the norm, which was written in **Homework 11.2**), its image corresponds to the class of:

$$x = \sum_{t \in G} t(1 \otimes f(s)) = \sum_{t \in G} t \otimes f(s)$$

2. Image of $s \cup f$: Using the property of cup products and boundary maps, we have $\delta(s \cup f) = \delta(s) \cup f$. Recall that in **Proposition 11.2**, $\hat{H}^{-2}(G; \mathbb{Z}) = H_1(G; \mathbb{Z}) \cong G^{ab} = G$ comes from:

$$H_1(G; \mathbb{Z}) \cong H_0(G; I_G) \cong I_G / I_G^2 \cong G^{ab} = G$$

So the element $s \in \hat{H}^{-2}(G, \mathbb{Z})$ maps under $\delta : \hat{H}^{-2}(G; \mathbb{Z}) \to \hat{H}^{-1}(G; I_G)$ to the class of $(s-1) \in \hat{H}^{-1}(G, I_G)$.

Suppose the "function form" of $\delta(s) \in \hat{H}^{-1}(G; I_G)$ is $\widetilde{\delta(s)}$: Or in another word, because $\hat{H}^{-1}(G; I_G) = \dfrac{\mathrm{Ker}(\mathrm{Hom}_G(\mathbb{Z}[G], I_G) \xrightarrow{\circ d^0} \mathrm{Hom}_G(\mathbb{Z}[G], I_G))}{\mathrm{Im}(\mathrm{Hom}_G(\mathbb{Z}[G^2], I_G) \xrightarrow{\circ d^{-1}} \mathrm{Hom}_G(\mathbb{Z}[G], I_G))}$, it can be lifted to an element of $\mathrm{Hom}_G(\mathbb{Z}[G], I_G)$, which is just $\widetilde{\delta(s)}$. In fact, $\widetilde{\delta(s)}$ corresponds to $s - 1 \in I_G$. Samely we can lift $f \in \mathrm{Hom}(G, A) = \hat{H}^1(G; A)$ to the function $\widetilde{f} \in \mathrm{Hom}_G(\mathbb{Z}[G^2], A)$.

Then $\delta(s) \cup f \in \hat{H}^0(G; I_G \otimes A)$ is lifted to the following function $\widetilde{\delta(s) \cup f} \in \mathrm{Hom}_G(\mathbb{Z}[G], I_G \otimes A)$, satisfying:

$$\begin{aligned}
\widetilde{\delta(s) \cup f}(1_G) &= (\widetilde{\delta(s)} \otimes \widetilde{f}) \circ \varphi_{-1,1}(1_G) \\
&= (\widetilde{\delta(s)} \otimes \widetilde{f}) \left(\sum_{t \in G} t \otimes (t, 1_G) \right) \\
&= \sum_{t \in G} \widetilde{\delta(s)}(t) \otimes \widetilde{f}(t, 1_G) \\
&= \sum_{t \in G} t(s-1) \otimes (tf(t^{-1})) \\
&= \sum_{t \in G} (t - ts) \otimes f(t)
\end{aligned}$$

So it corresponds to the obtained element in $I_G \otimes A$.

We expand the sum:

$$y = \sum_{t\in G} t \otimes f(t) - \sum_{t\in G} ts \otimes f(t).$$

In the second term, let $u = ts$. As t runs through G, so does u. Then $t = us^{-1}$. Since f is a homomorphism (trivial action), $f(t) = f(us^{-1}) = f(u) - f(s)$. Substituting this back:

$$\begin{aligned}\sum_{t\in G} ts \otimes f(t) &= \sum_{u\in G} u \otimes (f(u) - f(s)) \\ &= \sum_{u\in G} u \otimes f(u) - \sum_{u\in G} u \otimes f(s).\end{aligned}$$

Therefore,

$$y = \sum_{t\in G} t \otimes f(t) - \left(\sum_{u\in G} u \otimes f(u) - \sum_{u\in G} u \otimes f(s)\right) = \sum_{u\in G} u \otimes f(s).$$

Conclusion: We see that $x = y$ in $I_G \otimes A$, and thus their classes coincide in $\hat{H}^0(G, I_G \otimes A)$. Since δ is an isomorphism, we conclude that $s \cup f = f(s)$ in $\hat{H}^{-1}(G, A)$. □

12 2025.11.27

Proposition 12.1 (**Properties of cup products**).

(1) **Associativity:** If we identify $(A \otimes B) \otimes C$ with $A \otimes (B \otimes C)$, then

$$\alpha \cup (\beta \cup \gamma) = (\alpha \cup \beta) \cup \gamma$$

$\forall \alpha \in \hat{H}^p(G, A)$, $\beta \in \hat{H}^q(G, B)$, $\gamma \in \hat{H}^r(G, C)$.

(2) **Anticommutativity:** Identify $A \otimes B \cong B \otimes A$. Then

$$\alpha \cup \beta = (-1)^{pq}(\beta \cup \alpha)$$

$\forall \alpha \in \hat{H}^p(G, A)$, $\beta \in \hat{H}^q(G, B)$.

(3) Let $H \leq G$, $A, B \in \mathrm{Mod}_G$.

$$\mathrm{Res}^G_H(\alpha \cup \beta) = \mathrm{Res}^G_H(\alpha) \cup \mathrm{Res}^G_H(\beta)$$

$\forall \alpha \in \hat{H}^p(G, A)$, $\beta \in \hat{H}^q(G, B)$.

(4) Let $H \trianglelefteq G$, $A, B \in \mathrm{Mod}_G$.

$$\mathrm{Inf}(\alpha \cup \beta) = \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta) \quad \forall \alpha \in \hat{H}^p(G/H, A^H), \beta \in \hat{H}^q(G/H, B^H), p, q \geq 0.$$

(5) Let $H \leq G$.

$$\mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) = \mathrm{Cor}(\alpha) \cup \beta \quad \forall \alpha \in \hat{H}^p(H, A), \beta \in \hat{H}^q(G, B).$$

Idea of proof. Dimension shifting.

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}^G_{\{e\}} A \longrightarrow Q \longrightarrow 0$$

exact sequence of G-modules, split as $\mathbb{Z}$-modules (which implies $\otimes_{\mathbb{Z}} B$ is still exact). Then shifting to lower degrees.

$$0 \longrightarrow Q \longrightarrow \mathrm{ind}^G_{\{e\}} A \longrightarrow A \longrightarrow 0$$

exact sequence of G-modules, split as $\mathbb{Z}$-module. Then shifting to greater degrees.

So we may reduce to $\hat{H}^0$ case! Then check directly. □

12.1 Cohomology of finite cyclic group

G finite cyclic.

Theorem 12.1. $\forall A \in \mathrm{Mod}_G$, $\hat{H}^n(G,A) \cong \hat{H}^{n+2}(G,A)$ for all $n \in \mathbb{Z}$.

Proof. Idea: Construct a 2-periodic complete resolution of $\mathbb{Z}$. $G = \langle s \rangle$.

$$\cdots \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{\quad N \quad} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \cdots$$
$$\varepsilon \searrow \qquad \nearrow \varepsilon^*$$
$$\mathbb{Z}$$

where

$$N = \text{multiplying } \sum_{g \in G} g$$
$$D = \text{multiplying } s - 1$$

This is a complete resolution of $\mathbb{Z}$. Then the result follows from the definition of Tate cohomology. □

Remark: The isomorphism in the theorem depends on the choice of a generator $s \in G$.

Exercise 12.1. $\chi_s : G \to \mathbb{Q}/\mathbb{Z} : s^i \longmapsto \frac{i}{n}$ where $|G| = n$.

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta, \simeq} H^2(G, \mathbb{Z})$$
$$\chi_s \longmapsto \delta\chi_s$$

Show that for all $i \in \mathbb{Z}$, $- \cup \delta\chi_s : \hat{H}^i(G,A) \to \hat{H}^{i+2}(G,A)$ is the isomorphism.

Remark: $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ comes from the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and the fact that $H^i(G, \mathbb{Q}) = 0$ for all $i > 0$. We have proved it in **Homework 10.1**.

Definition 12.1. Suppose $\hat{H}^0(G,A)$ and $\hat{H}^1(G,A)$ are finite. Define **Herbrand quotient**:

$$h(A) := \frac{|\hat{H}^0(G,A)|}{|\hat{H}^1(G,A)|} \in \mathbb{Q}$$

Theorem 12.2.

(1) Let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. If two Herbrand quotients among $h(A), h(B), h(C)$ are defined, then so is the third, and we have $h(B) = h(A) \cdot h(C)$.

(2) If A is a finite G-module, then $h(A) = 1$.

(3) If f is a homomorphism of G-modules with finite kernel and cokernel. If one of the Herbrand quotient $h(A), h(B)$ is defined, then so is the other and $h(A) = h(B)$.

Proof. (1) We have the following exact sequence of Tate cohomology:

$$\begin{array}{ccccc} \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & \longrightarrow & \hat{H}^0(G,C) \\ {\scriptstyle\delta}\uparrow & & & & \downarrow{\scriptstyle\delta} \\ \hat{H}^1(G,C) & \longleftarrow & \hat{H}^1(G,B) & \longleftarrow & \hat{H}^1(G,A) \end{array}$$

The first statement follows immediately from the diagram. The second statement follows from the fact:

$$|\hat{H}^0(G,A)| \cdot |\hat{H}^1(G,B)| \cdot |\hat{H}^0(G,C)| = |\hat{H}^1(G,A)| \cdot |\hat{H}^0(G,B)| \cdot |\hat{H}^1(G,C)|$$

(2) $0 \to A^G \to A \xrightarrow{D} A \to A_G \to 0$ exact. Because A is finite, we will have $|A^G| = |A_G|$. From $0 \to \hat{H}^{-1}(G,A) \to A_G \xrightarrow{N} A^G \to \hat{H}^0(G,A) \to 0$ exact, we will have $|\hat{H}^0(G,A)| = |\hat{H}^{-1}(G,A)|$ and they are finite. So $h(A) = 1$.

(3) If $h(A)$ is defined, $0 \to \ker f \to A \xrightarrow{f} f(A) \to 0$ exact and from (1) and (2), $h(A) = h(f(A)) \cdot h(\ker f) = h(f(A))$. Also $0 \to f(A) \to B \to \mathrm{coker} f \to 0$ exact, so $h(B) = h(f(A)) \cdot h(\mathrm{coker} f) = h(f(A)) = h(A)$. If $h(B)$ is defined, similarly we have $h(A) = h(B)$. □

12.2 Cohomologically Trivial Module

Lemma 12.1. G is a p-group. $A \in \mathrm{Mod}_G$, $pA = 0$. Then the following are equivalent: (1) $A = 0$. (2) $A^G = 0$. (3) $A_G = 0$.

Proof. (1) $\implies$ (2), (3) trivial.

(2) $\implies$ (1). We first prove the case A is finite. From the orbital-stabilizer theorem,

$$|A^G| \equiv |A| \pmod{p}$$

Because $pA = 0$, A can be considered as a $\mathbb{F}_p$-vector space. So $|A|$ is a power of p. If $A^G = 0$, then $|A^G| = 1$. Contradiction! You can prove the general case from the finite case.

(3) $\implies$ (1). We use the following fact:

$$(A^\vee)^G \cong \mathrm{Hom}_G(A, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{F}_p}(A_G, \mathbb{F}_p)$$

If $A_G = 0$, then $(A^\vee)^G = 0$. By (2) $\implies$ (1), $A^\vee = 0$. So $A = 0$. □

Lemma 12.2. G: p-group. $pA = 0$. $H_1(G, A) = 0$. Then A is a free $\mathbb{F}_p[G]$-module.

Proof. Let $\{h_\lambda\} \in A_G$ be a $\mathbb{F}_p$-basis of A_G. Let $a_\lambda \in A$ be a lifting of h_λ.

Step 1: A is generated by $\{a_\lambda\}$ as $\mathbb{F}_p[G]$-module. Let $A' \subseteq A$ be the submodule generated by $\{a_\lambda\}$. Want to show $A' = A$.

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A/A' \longrightarrow 0$$

$$\Rightarrow (A')_G \longrightarrow A_G \longrightarrow (A/A')_G \longrightarrow 0$$

So $(A/A')_G = 0$. By **Lemma 12.1** $A/A' = 0$.

Step 2: A is free. Let L be the free $\mathbb{F}_p[G]$-module with basis e_λ.

$$0 \longrightarrow \ker\varphi \longrightarrow L \xrightarrow{\varphi} A \longrightarrow 0$$

$$\Rightarrow \underbrace{H_1(G, A)}_{0} \longrightarrow (\ker\varphi)_G \longrightarrow L_G \longrightarrow A_G \longrightarrow 0$$

We have $L_G \cong \bigoplus_\lambda \mathbb{F}_p e_\lambda$. (This is because $\mathbb{F}_p[G]_G \cong \mathbb{F}_p$ via deg) So $(\ker\varphi)_G = 0$, By **Lemma 12.1** $\ker\varphi = 0$. i.e. A is free. □

Definition 12.2. $A \in \mathrm{Mod}_G$ is called **cohomologically trivial** if $\hat{H}^n(H, A) = 0$ for all $H \leq G$ and all $n \in \mathbb{Z}$.

Example 12.1. If $A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} A_0$ is induced, then A is cohomologically trivial. (Reason: A is also induced as H-module as $\mathbb{Z}[G]$ is free $\mathbb{Z}[H]$-module).

Proposition 12.2. Let G be a p-group. $A \in \mathrm{Mod}_G$. $pA = 0$. Then the following are equivalent:

1. There exists $q \in \mathbb{Z}$ such that $\hat{H}^q(G, A) = 0$.
2. A is cohomologically trivial.
3. A is (co-)induced.
4. A is free $\mathbb{F}_p[G]$-module.

Proof. (3) $\Rightarrow$ (2) $\Rightarrow$ (1). ✓

(4) $\Rightarrow$ (3). $A \cong \mathbb{F}_p[G] \otimes_{\mathbb{F}_p} M \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$.

(1) $\Rightarrow$ (4). By dimension shifting, there exists $B \in \mathrm{Mod}_G$ such that for all $n \in \mathbb{Z}$:

$$\hat{H}^n(G, A) = \hat{H}^{n-q-2}(G, B)$$

Moreover $pB = 0$ as $pM = 0$ implies $p \cdot \mathrm{ind}_1^G M$ implies $p \cdot \ker(\mathrm{ind}_1^G M \to M) = 0$. Hence $H_1(G, B) = \hat{H}^{-2}(G, B) \cong \hat{H}^q(G, A) = 0$. By **Lemma 12.2**, B is a free $\mathbb{F}_p[G]$-module and hence cohomologically trivial. Hence $H_1(G, A) = \hat{H}^{-2}(G, A) = \hat{H}^{-q-4}(G, B) = 0$. Apply **Lemma 12.2** again. □

Proposition 12.3. $A \in \mathrm{Mod}_G$. If for all prime number p, there exists $q \in \mathbb{Z}$ (depending on p) such that

$$\hat{H}^q(G_p, A) = \hat{H}^{q+1}(G_p, A) = 0$$

where G_p is a p-Sylow of G. Then A is cohomologically trivial.

Proof. Write $0 \longrightarrow R \longrightarrow F \longrightarrow A \longrightarrow 0$, where F is free $\mathbb{Z}[G]$-module in particular relatively injective. Then:

$$\hat{H}^{q+1}(G_p, R) = \hat{H}^q(G_p, A) = 0 = \hat{H}^{q+1}(G_p, A) = \hat{H}^{q+2}(G_p, R)$$

Consider the exact sequence

$$0 \longrightarrow R \xrightarrow{p} R \longrightarrow R/pR \longrightarrow 0$$

This implies that $\hat{H}^{q+1}(G_p, R/pR) = 0$. By **Proposition 12.2**, R/pR is a free $\mathbb{F}_p[G_p]$-module and simultaneously an induced G_p-module.

Case 1: A is free over $\mathbb{Z}$. Let $M := \mathrm{Hom}_{\mathbb{Z}}(A, R)$.

Claim 1: $H^1(G, M) = 0$. Since A is free over $\mathbb{Z}$, the functor $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ is exact. Applying this to the sequence above, we get:

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, R) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A, R) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, R/pR) \longrightarrow 0$$

which can be rewritten as:

$$0 \longrightarrow M \xrightarrow{p} M \longrightarrow M/pM \longrightarrow 0$$

This implies that M/pM is also an induced G_p-module.

Indeed, $R/pR \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_p], N)$ for some abelian group N. We have the following isomorphisms:

$$\begin{aligned} M/pM &\cong \mathrm{Hom}_{\mathbb{Z}}(A, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_p], N)) \\ &\cong \mathrm{Hom}_{\mathbb{Z}}(A \otimes_{\mathbb{Z}} \mathbb{Z}[G_p], N) \\ &\cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_p], \mathrm{Hom}_{\mathbb{Z}}(A, N)) \end{aligned}$$

Thus M/pM is (co-)induced, and hence cohomologically trivial G_p-module. This implies that the multiplication by p map:

$$\hat{H}^n(G_p, M) \xrightarrow{p} \hat{H}^n(G_p, M)$$

is an isomorphism for all n. Consequently, the p-torsion subgroup $\hat{H}^n(G_p, M)[p]$ is zero. Therefore, we conclude that $\hat{H}^n(G, M) = 0$. This follows because the restriction map

$$\mathrm{Res} : \hat{H}^n(G, M)[p] \longrightarrow \hat{H}^n(G_p, M)[p]$$

is injective from **Corollary 10.6**.

Claim 2: A is a direct factor of F.

$$0 \longrightarrow R \longrightarrow F \longrightarrow A \longrightarrow 0$$

Apply $\mathrm{Hom}_{\mathbb{Z}}(A, -)$:

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, R) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, F) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, A) \longrightarrow 0$$

Apply $(-)^G$:

$$0 \longrightarrow M^G \longrightarrow \mathrm{Hom}_G(A, F) \longrightarrow \mathrm{Hom}_G(A, A) \longrightarrow \underbrace{H^1(G, M)}_{=0}$$

Suppose $\theta \in \mathrm{Hom}_G(A, F)$ maps to $\mathrm{id} \in \mathrm{Hom}_G(A, A)$. Then θ is a splitting of the original exact sequence. i.e.:

$$0 \longrightarrow R \longrightarrow F \underset{\theta}{\overset{\longrightarrow}{\longleftarrow}} A \longrightarrow 0$$

So A is a direct factor of F.

From Claim 2 and F is relatively injective, A is cohomologically trivial. We've done Case 1.

Case 2: General case. F is free over $\mathbb{Z}$, so R is also free over $\mathbb{Z}$. Apply Case 1 to R. Then R is cohomologically trivial. Then easily know A is cohomologically trivial. □

Theorem 12.3 (**Tate-Nakayama Theorem**). $A \in \mathrm{Mod}_G$. $a \in H^2(G, A)$. Assume for all prime p:

(a) $H^1(G_p, A) = 0$.

(b) $H^2(G_p, A)$ is a cyclic group of order $|G_p|$ generated by $a_p = \mathrm{Res}\, a \in H^2(G_p, A)$.

Then for all $H \leq G$, the cup product by $a_H = \mathrm{Res}^G_H(a) \in H^2(H, A)$ induces isomorphism:

$$- \cup a_H : \hat{H}^n(H, \mathbb{Z}) \longrightarrow \hat{H}^{n+2}(H, A) \quad \forall n \in \mathbb{Z}.$$

Application to CFT

Local: $G = \mathrm{Gal}(L/K)$. L/K finite Galois extension of p-adic field. $A = L^*$, $n = -2$, $H = G$.

$$G^{\mathrm{ab}} = H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z}) \overset{\cong}{\to} \hat{H}^0(G, L^*) = K^*/N_{L/K}(L^*)$$

Global: $G = \mathrm{Gal}(L/K)$. L/K finite Galois extension of number fields. $A = C^*_L$.

Before proving Tate-Nakayama Theorem, we need the following proposition.

Proposition 12.4. Let $A, A' \in \mathrm{Mod}_G$. $f : A' \to A$ homomorphism of G-modules. Assume that for all prime p, there exists $n_p \in \mathbb{Z}$ such that:

$$f^i_* : \hat{H}^i(G_p, A') \longrightarrow \hat{H}^i(G_p, A)$$

is surjective for $i = n_p$, bijective for $i = n_p + 1$, injective for $i = n_p + 2$. Then $\hat{H}^i(H, A') \overset{f_*}{\to} \hat{H}^i(H, A)$ is bijective for all $n \in \mathbb{Z}$, for all $H \leq G$.

Proof. **Case 1:** f is injective. Consider $0 \longrightarrow A' \xrightarrow{f} A \longrightarrow A'' \longrightarrow 0$. It suffices to show A'' is cohomologically trivial.

We have the following exact sequence:

$$\begin{aligned}\ldots \longrightarrow \hat{H}^{n_p}(G_p, A') &\xrightarrow{\text{surjective}} \hat{H}^{n_p}(G_p, A) \xrightarrow{0} \hat{H}^{n_p}(G_p, A'') \\ &\xrightarrow{0} \hat{H}^{n_p+1}(G_p, A') \xrightarrow{\text{bijective}} \hat{H}^{n_p+1}(G_p, A) \xrightarrow{0} \hat{H}^{n_p+1}(G_p, A'') \\ &\xrightarrow{0} \hat{H}^{n_p+2}(G_p, A') \xrightarrow{\text{injective}} \hat{H}^{n_p+2}(G_p, A) \longrightarrow \hat{H}^{n_p+2}(G_p, A'') \longrightarrow \ldots\end{aligned}$$

So $\hat{H}^{n_p}(G_p, A'') = \hat{H}^{n_p+1}(G_p, A'') = 0$. From **Proposition 12.3**, A'' is cohomologically trivial.

Case 2: General case. $A' \xrightarrow{\widetilde{f}} A^* := A \oplus \mathrm{Ind}_1^G A'$ injective. Apply Case 1 to $\widetilde{f}$. □

Proof of Theorem.

$$\begin{aligned}0 \longrightarrow A \longrightarrow \mathrm{Ind}_1^G A \longrightarrow A_1 \longrightarrow 0 \\ 0 \longrightarrow A_1 \longrightarrow \mathrm{Ind}_1^G A_1 \longrightarrow A_2 \longrightarrow 0\end{aligned}$$

Let $B = A_2$. Then $\hat{H}^n(G, B) \xrightarrow{\delta^2} \hat{H}^{n+2}(G, A)$ is an isomorphism for all $n \in \mathbb{Z}$.

Consider $n = 0$, there exists $b \in \hat{H}^0(G, B)$, such that by the map δ^2, $b \mapsto a \in \hat{H}^2(G, A)$.

By the assumptions, for all prime p:

(a) $\hat{H}^{-1}(G_p, B) = 0$.

(b) $\hat{H}^0(G_p, B)$ is cyclic of order $|G_p|$ generated by $b_p = \mathrm{Res}\, b$.

Now construct: $\tilde{b} \in B$ is a lifting of $b \in \hat{H}^0(G, B)$. $f : \mathbb{Z} \to B : m \mapsto m\widetilde{b}$. Our goal is to show that for all prime p:

- $f_*^{-1} : \hat{H}^{-1}(G_p, \mathbb{Z}) \longrightarrow \hat{H}^{-1}(G_p, B)$ is surjective.
- $f_*^{0} : \hat{H}^{0}(G_p, \mathbb{Z}) \longrightarrow \hat{H}^{0}(G_p, B)$ is bijective.
- $f_*^{1} : \hat{H}^{1}(G_p, \mathbb{Z}) \longrightarrow \hat{H}^{1}(G_p, B)$ is injective.

If we prove this, then by **Proposition 12.4**, for all $H \leq G$, for all $n \in \mathbb{Z}$,

$$f_*^n : \hat{H}^n(H, \mathbb{Z}) \longrightarrow \hat{H}^n(H, B)$$

is an isomorphism. Notice that we have the following commutative diagram:

$$\begin{array}{ccc} \hat{H}^n(H,\mathbb{Z}) & \xrightarrow{-\cup a_H} & \hat{H}^{n+2}(H,A) \\ \| & & \uparrow{\scriptstyle \delta^2} \\ \hat{H}^n(H,\mathbb{Z}) & \xrightarrow{f_*^n} & \hat{H}^n(H,B) \end{array}$$

(This is because $* \cup a_H = * \cup \delta^2 b_H = \delta^2(* \cup b_H)$). So $- \cup a_H$ is an isomorphism for all $H \leq G$, for all $n \in \mathbb{Z}$.

- $\hat{H}^{-1}(G_p, B) = 0$, so f_*^{-1} is surjective.
- $\hat{H}^0(G_p, \mathbb{Z}) \cong \mathbb{Z}/|G_p|\mathbb{Z} \xrightarrow{f_*} \hat{H}^0(G_p, B)$ is actually $1 \mapsto b_p$, which is bijective since $\hat{H}^0(G_p, B)$ is cyclic of order $|G_p|$ generated by b_p.
- $\hat{H}^1(G_p, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G_p, \mathbb{Z}) = 0$, so f_*^1 is injective.

□

12.3 Homework

Homework 12.1. Let $G = \langle s \rangle$ be a cyclic group of order n. Let $\chi : G \to \mathbb{Q}/\mathbb{Z}$ be the group homomorphism s.t. $\chi(s) = \frac{1}{n}$. Let $\delta\chi$ be the image of χ via $\delta : \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G, \mathbb{Z})$. Then

$$- \cup \delta\chi : \hat{H}^i(G, A) \to \hat{H}^{i+2}(G, A).$$

is the isomorphism in the course.

Proof. It suffices to show the $i = -1$ case. Other case can be proved by dimension shifting.

Every element in $\hat{H}^{-1}(G, A)$ can be written as $[a] \in A_G$, where $a \in A$ such that $\sum_{g \in G} ga = 0$. χ can also be considered as homogeneous χ^{hol}, i.e.

$$\chi^{hol}(s^m, s^n) = \chi(s^{n-m}) = \frac{\overline{n-m}}{n} \in \mathbb{Q}/\mathbb{Z}$$

It can be lifted to $\widehat{\chi} \in \mathrm{Hom}_G(\mathbb{Z}[G^2], \mathbb{Q})$:

$$\widehat{\chi}(1, s^m) := \frac{m}{n} \quad (m = 0, 1, \ldots, n-1)$$

$[a] \cup \delta\chi \in \hat{H}^1(G, A)$ can be lifted to a function $\phi : G \to A$ such that $\phi(g_1 g_2) = g_1\phi(g_2) + \phi(g_2)$. Now we compute for $m = 1, \ldots, n-1$:

$$\begin{aligned}
\phi(s^m) &= ([a] \otimes \delta\chi) \circ \varphi_{-1,2}(1, s^m) \\
&= ([a] \otimes \delta\chi)(\sum_{i=0}^{n-1} s^i \otimes (s^i, 1, s^m)) \\
&= \sum_{i=0}^{n-1} s^i a \cdot \widehat{\chi}(s^i, 1, s^m) \\
&= \sum_{i=0}^{n-1} s^i a \cdot \chi^{hol} \circ d(s^i, 1, s^m) \\
&= \sum_{i=1}^{m} \frac{m - (m-i) + (n-i)}{n} s^i a + \sum_{i=m+1}^{n-1} \frac{m - (n + (m-i)) + (n-i)}{n} s^i a \\
&= \sum_{i=1}^{m} s^i a
\end{aligned}$$

Now we have discribed how the cup product works:

$$\begin{aligned} -\cup\delta\chi : \hat{H}^{-1}(G,A) &\to \hat{H}^1(G,A) \\ [a] &\mapsto \left[g \mapsto \sum_{i=1}^{m} s^i a \text{ for } g = s^m, m = 1,\dots,n-1 \right] \end{aligned}$$

Consider the G-module homomorphism $j : \mathbb{Z}[G] \to \mathbb{Z}[G^2] : s^l \mapsto (s^l, s^{l+1})$, then we have the following commutative diagram:

$$\begin{array}{ccccccccccc} \cdots & \xrightarrow{D} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{D} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{D} & \cdots \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle j} & & \| & & \| & & \\ \cdots & \xrightarrow{d} & \mathbb{Z}[G^3] & \xrightarrow{d} & \mathbb{Z}[G^2] & \xrightarrow{d} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{d^*} & \cdots \end{array}$$

Denote the complete resolution of $\mathbb{Z}$ in the first row by $P_\bullet$, second by $Q_\bullet$. Then the following isomorphism is induced by composing with j:

$$\beta : H^1(\mathrm{Hom}_G(Q_\bullet, A)) \xrightarrow{\cong} H^1(\mathrm{Hom}_G(P_\bullet, A))$$

Denote $\alpha := (-\cup\delta\chi) : H^{-1}(\mathrm{Hom}_G(Q_\bullet, A)) = H^{-1}(\mathrm{Hom}_G(P_\bullet, A)) \to H^1(\mathrm{Hom}_G(Q_\bullet, A))$. From $P_\bullet$ we know $H^{-1}(\mathrm{Hom}_G(P_\bullet, A)) = H^1(\mathrm{Hom}_G(P_\bullet, A))$. Our main goal is to show that $\beta \circ \alpha = \mathrm{id}$.

For any $[a] \in H^{-1}(\mathrm{Hom}_G(P_\bullet, A))$, $\beta \circ \alpha([a])$ can be lifted to the following element in A:

$$(\beta \circ \alpha([a]))_{\mathrm{lift}}(1) = \alpha([a])_{\mathrm{lift}}(j(1)) = \phi^{hol}(1, s) = \phi(s) = sa$$

Note that $[a] = [sa] \in A_G$, so $\beta \circ \alpha = \mathrm{id}$. □

Homework 12.2. Let G be a finite cyclic group. Compute the Herbrand quotient $h(\mathbb{Z})$ for the trivial G-module $\mathbb{Z}$.

Solution. Let $n = |G|$ be the order of the group. Since G is cyclic, let $G = \langle\sigma\rangle$. The Herbrand quotient is defined as:

$$h(\mathbb{Z}) = \frac{|\hat{H}^0(G,\mathbb{Z})|}{|\hat{H}^1(G,\mathbb{Z})|}$$

Recall: **Example 11.1**.

Step 1: Compute $\hat{H}^0(G,\mathbb{Z})$

By the definition of Tate cohomology:

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

Since $\mathbb{Z}$ is a trivial G-module, the action of G is the identity. Thus, the invariants are the whole group:

$$\mathbb{Z}^G = \{m \in \mathbb{Z} \mid \sigma m = m\} = \mathbb{Z}$$

The norm map $N : \mathbb{Z} \to \mathbb{Z}$ is defined by $N(m) = \sum_{g\in G} g \cdot m$. Since the action is trivial:

$$N(m) = \sum_{i=1}^{n} m = n \cdot m$$

Thus, $N_G\mathbb{Z} = n\mathbb{Z}$. Therefore:

$$\hat{H}^0(G,\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \implies |\hat{H}^0(G,\mathbb{Z})| = n$$

Step 2: Compute $\hat{H}^1(G,\mathbb{Z})$

For a finite group G, the first Tate cohomology group is isomorphic to the standard group cohomology:

$$\hat{H}^1(G,\mathbb{Z}) \cong H^1(G,\mathbb{Z})$$

Since the action is trivial, $H^1(G,\mathbb{Z})$ is the group of group homomorphisms from G to $\mathbb{Z}$:

$$H^1(G,\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{group}}(G,\mathbb{Z})$$

Since G is a finite group, every element in G has finite order. However, $\mathbb{Z}$ is a torsion-free group (the only element with finite order is 0). Therefore, any homomorphism $f : G \to \mathbb{Z}$ must map every element to 0.

$$\mathrm{Hom}(G,\mathbb{Z}) = 0 \implies |\hat{H}^1(G,\mathbb{Z})| = 1$$

Step 3: Compute the Quotient

$$h(\mathbb{Z}) = \frac{n}{1} = n$$

Conclusion: The Herbrand quotient is $h(\mathbb{Z}) = |G|$.

□

Homework 12.3. Let G be a finite cyclic group, and let V be a finite dimensional real vector space on which G acts linearly (i.e., V is an $\mathbb{R}[G]$-module). Let M and N be two G-stable lattices in V.

(a) Show that $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq N \otimes_{\mathbb{Z}} \mathbb{Q}$ as $\mathbb{Q}[G]$-modules;

(b) Show that if either $h(M)$ or $h(N)$ is defined, then so is the other, and they are equal.

Proof of (a). Let $V_M = M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $V_N = N \otimes_{\mathbb{Z}} \mathbb{Q}$. These are finite-dimensional representations of G over $\mathbb{Q}$. Since M is a lattice in V, we have an isomorphism of $\mathbb{R}[G]$-modules:

$$V_M \otimes_{\mathbb{Q}} \mathbb{R} \cong M \otimes_{\mathbb{Z}} \mathbb{R} \cong V$$

Similarly, for N, we have:

$$V_N \otimes_{\mathbb{Q}} \mathbb{R} \cong N \otimes_{\mathbb{Z}} \mathbb{R} \cong V$$

Thus, $V_M \otimes_{\mathbb{Q}} \mathbb{R} \cong V_N \otimes_{\mathbb{Q}} \mathbb{R}$ as $\mathbb{R}[G]$-modules.

For a finite group G and a field K of characteristic 0 (here $K = \mathbb{Q}$), a representation is determined up to isomorphism by its character. Let χ_M and χ_N be the characters of V_M and V_N respectively. The character of the extended representation $V_M \otimes \mathbb{R}$ is the same as χ_M (viewed as a function $G \to \mathbb{R}$).

Since $V_M \otimes \mathbb{R} \cong V_N \otimes \mathbb{R}$, their characters are equal:

$$\chi_M(g) = \chi_N(g) \quad \text{for all } g \in G.$$

Since the characters are equal, the rational representations V_M and V_N are isomorphic as $\mathbb{Q}[G]$-modules. □

Proof of (b). From part (a), there exists a $\mathbb{Q}[G]$-module isomorphism:

$$\Phi : M \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} N \otimes_{\mathbb{Z}} \mathbb{Q}$$

We can view M as a subset of $M \otimes \mathbb{Q}$ via $m \mapsto m \otimes 1$, and similarly for N. Since M is a finitely generated $\mathbb{Z}$-module, its image $\Phi(M)$ is a finitely generated $\mathbb{Z}$-submodule of $N \otimes \mathbb{Q}$.

Since N is a lattice in $N \otimes \mathbb{Q}$, it spans the space. Therefore, there exists a non-zero integer k such that

$$k \cdot \Phi(M) \subseteq N$$

(Reason: Since M is a lattice, it is a finitely generated free $\mathbb{Z}$-module. Let $\{e_1, \ldots, e_r\}$ be a basis of M. For each basis element e_i, since $\Phi(e_i) \in N \otimes_{\mathbb{Z}} \mathbb{Q}$, there exists a non-zero integer d_i such that $d_i\Phi(e_i) \in N$. By taking k to be the product (or least common multiple) of all d_i, we ensure that $k\Phi(e_i) \in N$ for all i, which implies $k\Phi(M) \subseteq N$.)

Let $f : M \to N$ be the map defined by $f(m) = k \cdot \Phi(m)$. Since Φ is G-linear and multiplication by k is G-linear (as the action is linear), f is a homomorphism of G-modules.

We analyze the kernel and cokernel of f:

- **Kernel:** Since Φ is an isomorphism and V is torsion-free, $f(m) = 0 \implies m = 0$. Thus, $\ker(f) = 0$, which is finite.
- **Cokernel:** M and N are lattices of the same rank (equal to $\dim_{\mathbb{R}} V$). The image $f(M)$ is a sublattice of N of full rank. Therefore, the quotient group $N/f(M)$ is finite. Thus, $\operatorname{coker}(f)$ is finite.

According to **Theorem 12.2 (3)** in the notes: If $f : M \to N$ is a homomorphism of G-modules with finite kernel and cokernel, and if the Herbrand quotient of one of them is defined, then so is the other, and $h(M) = h(N)$.

Since we constructed such a map f, the result follows. □

Homework 12.4. Let L/K be a finite extension of number fields with cyclic Galois group G. Let $V_{K,\infty} \subset S \subset V_K$ be a finite set of primes of K, and let $\tilde{S}$ be the set of primes of L lying over a prime of K in S. Let

$$\mathcal{O}^*_{L,\tilde{S}} = \{x \in L \mid \|x\|_w = 1, \forall w \notin \tilde{S}\}.$$

Then G acts on $\tilde{S}$ and $\mathcal{O}^*_{L,\tilde{S}}$.

(a) Let V be a product of copies of $\mathbb{R}$ indexed by the elements of $\tilde{S}$, i.e., $V = \operatorname{Hom}(\tilde{S}, \mathbb{R})$. Define the action of G on V by $(\sigma f)(w) = f(\sigma^{-1}w)$ for any $\sigma \in G$ and $w \in \tilde{S}$. Define the lattice $N = \operatorname{Hom}(\tilde{S}, \mathbb{Z})$ in V. Show that $h(N) = \prod_{v \in S} n_v$ where $n_v = [L_w : K_v]$ for any place w of L over v.

(b) Define $\theta : \mathcal{O}^*_{L,\tilde{S}} \to V, x \mapsto f_x$ where $f_x(w) = \log(\|x\|_w)$ for all $w \in \tilde{S}$. Let M^0 be the image of θ. Show that $h(\mathcal{O}^*_{L,\tilde{S}}) = h(M^0)$.

(c) Let $M = M^0 + \mathbb{Z}e$ where $e \in V$ is the constant function with value 1. Show that $h(\mathcal{O}^*_{L,\tilde{S}}) = \frac{\prod_{v \in S} n_v}{n}$, where $n = |G|$. (Hint: Compute $h(M)$ and apply previous exercise).

Proof of (a). The set $\tilde{S}$ is a G-set. The action of G partitions $\tilde{S}$ into disjoint orbits. These orbits are in one-to-one correspondence with the primes $v \in S$ of K. For each $v \in S$, let $\tilde{S}_v = \{w \in \tilde{S} \mid w|v\}$ be the set of primes in L lying above v.

The lattice $N = \mathrm{Hom}(\tilde{S}, \mathbb{Z})$ is the free abelian group generated by the elements of $\tilde{S}$. Therefore, we have a decomposition of N as a direct sum of G-modules:

$$N = \bigoplus_{v \in S} N_v, \quad \text{where } N_v = \bigoplus_{w \in \tilde{S}_v} \mathbb{Z}w.$$

By the multiplicative property of the Herbrand quotient (**Theorem 12.2 (1)**), we have:

$$h(N) = \prod_{v \in S} h(N_v).$$

Fix a prime $v \in S$ and choose a prime $w \in \tilde{S}_v$ lying above it. Let $G_w = \{\sigma \in G \mid \sigma w = w\}$ be the decomposition group of w. The orbit $\tilde{S}_v$ is isomorphic to the coset space G/G_w as a G-set. Thus, the module N_v is isomorphic to the induced module:

$$N_v \cong \mathrm{Ind}_{G_w}^{G}(\mathbb{Z}),$$

where $\mathbb{Z}$ is the trivial G_w-module.

By Shapiro's Lemma (generalized to Tate cohomology, **Homework 11.3**), we have an isomorphism $\hat{H}^i(G, \mathrm{Ind}_{G_w}^{G}\mathbb{Z}) \cong \hat{H}^i(G_w, \mathbb{Z})$. Therefore:

$$h(N_v) = h_G(\mathrm{Ind}_{G_w}^{G}\mathbb{Z}) = h_{G_w}(\mathbb{Z}).$$

From **Homework 12.2**, for a cyclic group H acting trivially on $\mathbb{Z}$, the Herbrand quotient is $h(\mathbb{Z}) = |H|$. Here, the group is G_w, and its order is the local degree $n_v = [L_w : K_v]$. Thus:

$$h(N_v) = |G_w| = n_v.$$

Substituting this back into the product:

$$h(N) = \prod_{v \in S} n_v.$$

□

Proof of (b). Consider the homomorphism $\theta : \mathcal{O}_{L,\tilde{S}}^{*} \to V$. Its image is M^0. The kernel of

θ is:

$$\ker(\theta) = \{x \in \mathcal{O}_{L,\tilde{S}}^* \mid \log(\|x\|_w) = 0, \forall w \in \tilde{S}\} = \{x \in \mathcal{O}_{L,\tilde{S}}^* \mid \|x\|_w = 1, \forall w \in \tilde{S}\}.$$

Since x is an S-unit, $\|x\|_v = 1$ for all $v \notin \tilde{S}$. Thus, elements in the kernel have absolute value 1 at all places of L. It is well-known that $\ker(\theta)$ consists of the roots of unity in L, denoted μ_L.

We have the exact sequence of G-modules:

$$0 \longrightarrow \mu_L \longrightarrow \mathcal{O}_{L,\tilde{S}}^* \xrightarrow{\theta} M^0 \longrightarrow 0.$$

Since μ_L is a finite group, by **Theorem 12.2 (2)**, its Herbrand quotient is $h(\mu_L) = 1$. Using the multiplicative property of Herbrand quotients for exact sequences (**Theorem 12.2 (1)**):

$$h(\mathcal{O}_{L,\tilde{S}}^*) = h(\mu_L) \cdot h(M^0) = 1 \cdot h(M^0) = h(M^0).$$

□

Proof of (c). Let $e \in V$ be the function $e(w) = 1$ for all $w \in \tilde{S}$. The action of G on e is trivial because G permutes the domain $\tilde{S}$:

$$(\sigma e)(w) = e(\sigma^{-1}w) = 1 = e(w).$$

Thus, the lattice $\mathbb{Z}e$ is isomorphic to the trivial G-module $\mathbb{Z}$.

By the Product Formula, for any unit $u \in \mathcal{O}_{L,\tilde{S}}^*$, we have $\sum_{w \in \tilde{S}} \log \|u\|_w = 0$. This means that every element $f \in M^0$ satisfies $\sum_w f(w) = 0$. However, for the element e, $\sum_w e(w) = |\tilde{S}| \neq 0$. Therefore, $M^0 \cap \mathbb{Z}e = \{0\}$.

We have a direct sum decomposition of G-modules:

$$M = M^0 \oplus \mathbb{Z}e.$$

(Note: **Dirichlet's S-Unit Theorem** ensures M^0 has rank $|\tilde{S}| - 1$, so M has rank $|\tilde{S}|$ and is a lattice in V).

Using the multiplicative property:

$$h(M) = h(M^0) \cdot h(\mathbb{Z}e).$$

From **Homework 12.2**, since G acts trivially on $\mathbb{Z}e \cong \mathbb{Z}$, we have $h(\mathbb{Z}e) = |G| = n$.

Now, compare the two lattices M and N in the representation V. Both are G-stable lattices in the same $\mathbb{R}[G]$-module V. According to **Homework 12.3 (b)**, their Herbrand quotients must be equal:

$$h(M) = h(N).$$

From part (a), we know $h(N) = \prod_{v \in S} n_v$. Substituting these into the equation for $h(M)$:

$$\prod_{v \in S} n_v = h(M^0) \cdot n.$$

Solving for $h(M^0)$:

$$h(M^0) = \frac{1}{n} \prod_{v \in S} n_v.$$

Finally, using the result from part (b):

$$h(\mathcal{O}^*_{L,\tilde{S}}) = h(M^0) = \frac{\prod_{v \in S} n_v}{n}.$$

□

13 2025.12.4

VI. Proof of Local Class Field Theory

13.1 Galois cohomology

Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$, $A = L$ or L^*.

Proposition 13.1. $\hat{H}^n(G, L) = 0, \forall n \in \mathbb{Z}$ (i.e. L is cohomologically trivial).

Proof. By **Normal Basis Theorem**, there exists $\beta \in L$ such that $\{g\beta\}_{g\in G}$ forms a K-basis of L. So $L \cong K[G]$ as G-module:

$$L \cong K[G] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} K = \mathrm{ind}_1^G K.$$

Hence L is cohomologically trivial. □

Theorem 13.1 (**Hilbert 90**). $H^1(G, L^*) = 0$.

Proof. Let $f \in Z^1(G, L^*) : G \to L^*$, i.e. $f(g_1g_2) = (g_1 f(g_2)) \cdot f(g_1)$. We want to show $f \in B^1(G, L^*)$, i.e. there exists $b \in L^*$ s.t. $f(g) = \frac{gb}{b}$.

By **Dedekind's theorem**, $g \in G$, $g : L^* \to L^*$ are linearly independent. So there exists $c \in L^*$ such that:

$$\sum_{g\in G} f(g)g(c) \neq 0$$

We set:

$$b := \left(\sum_{g\in G} f(g)g(c)\right)^{-1}$$

For any $g \in G$,

$$g(b^{-1}) = \sum_{\tilde{g}\in G} g(f(\tilde{g}))g\tilde{g}(c) = \sum_{\tilde{g}\in G} \frac{f(g\tilde{g})}{f(g)} g\tilde{g}(c) = \frac{1}{f(g)} \sum_{\hat{g}\in G} f(\hat{g})\hat{g}(c) = \frac{b^{-1}}{f(g)}$$

So:

$$f(g) = \frac{g(b)}{b}$$

□

Definition 13.1. Let G be a profinite group. A **discrete G-module** is a G-module A such that

$$A = \bigcup_{\substack{H \leq G \\ \text{open}}} A^H$$

(Note: A^H is a G/H-module). Let Mod_G^d be the category of discrete G-modules.

Definition 13.2. Let $A \in \mathrm{Mod}_G^d$.

$$H^n(G, A) := \varinjlim_{H \trianglelefteq G \text{ open}} H^n(G/H, A^H)$$

where the transition maps are

$$\mathrm{Inf} : H^n(G/H, A^H) \longrightarrow H^n(G/H', A^{H'}), \quad H' \subseteq H.$$

Remark: Indeed $H^i(G, A)$ can also be defined as the derived functor of the left exact functor $(-)^G : \mathrm{Mod}_G^d \to \mathrm{Mod}_G^d$.

Definition 13.3. Let $H \leq G$ be a closed subgroup. Define the **continuous co-induction functor** $\text{c-Ind}_H^G : \mathrm{Mod}_H^d \longrightarrow \mathrm{Mod}_G^d$ by

$$A \longmapsto \text{c-Ind}_H^G A := \{f : G \to A \text{ continuous } \mid f(hg) = hf(g), \forall h \in H\}$$

Exercise 13.1.

(1) c-Ind(A) is indeed a discrete G-module.

(2) We have the adjunction formula:

$$\mathrm{Hom}_H(\mathrm{Res}_H^G A, A') \cong \mathrm{Hom}_G(A, \text{c-Ind}_H^G A')$$

In particular, c-Ind preserves injectives.

Lemma 13.1. Mod_G^d has enough injective objects.

Proof. For all $A \in \mathrm{Mod}_G^d$, there exists an injective $\mathbb{Z}$-module I such that A can be embedded into I. Consider:

$$A \hookrightarrow \text{c-Ind}_1^G A \hookrightarrow \text{c-Ind}_1^G I$$

Because c-$\mathrm{Ind}_1^G -$ preserves injectives, we are done. □

Remark: Mod_G^d in general doesn't have enough projective objects.

Example 13.1 (**Examples of discrete G-modules**).

1. $\mathbb{Z}[G]$ is **not** discrete.
2. $G = \mathrm{Gal}(\overline{K}/K)$. $A = \overline{K}$ or $\overline{K}^*$ ($\overline{K} \triangleq K^{\mathrm{sep}}$).
3. G is a profinite group, $H \trianglelefteq G$ is open. Let $A \in \mathrm{Mod}_{G/H}$. Then $f^*A \in \mathrm{Mod}_G^d$, where $f : G \to G/H$ is the quotient map.

Definition 13.4.

1. Let K be a field. Let A be a discrete $\mathrm{Gal}(\overline{K}/K)$-module.
$$H^i(K, A) := H^i(\mathrm{Gal}(\overline{K}/K), A)$$
2. Let L/K be a finite extension. Let $A \in \mathrm{Mod}_{\mathrm{Gal}(L/K)}$. Define:
$$H^i(L/K, A) := H^i(\mathrm{Gal}(L/K), A)$$

Corollary 13.1.

1. $H^q(K, \overline{K}) = 0$ for all $q > 0$.
2. $H^1(K, \overline{K}^*) = 0$.
3. Let $n > 0$ such that $\mathrm{char}(K) \nmid n$. Let μ_n be the multiplicative group of n-th roots of unity in $\overline{K}$. Then $K^*/K^{*n} \cong H^1(K, \mu_n)$.

Proof. (1) and (2) have been proven.

(3) Consider the exact sequence:
$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow{(\cdot)^n} \overline{K}^* \longrightarrow 1$$

This induces the long exact sequence:
$$\cdots \longrightarrow K^* \xrightarrow{(\cdot)^n} K^* \longrightarrow H^1(K, \mu_n) \longrightarrow H^1(K, \overline{K}^*) = 0$$

Here we used $H^0(K, \overline{K}^*) = (\overline{K}^*)^{\mathrm{Gal}(\overline{K}/K)} = K^*$. Thus, we obtain the isomorphism $K^*/K^{*n} \cong H^1(K, \mu_n)$. □

Definition 13.5.

1. $\mathrm{Br}(K) := H^2(K, \overline{K}^*)$ is called the **Brauer group**.
2. For a finite Galois extension L/K, we define $\mathrm{Br}(L/K) := H^2(L/K, L^*)$.

Remark:

1. $\mathrm{Br}(K) = \varinjlim_{L/K \text{ fin Galois}} \mathrm{Br}(L/K)$ with transition maps.
   The transition map is inflation: $\mathrm{Inf} : \mathrm{Br}(L_1/K) \to \mathrm{Br}(L_2/K)$ with $L_1 \subseteq L_2$.
   Indeed, we have the exact sequence:
   $$0 \longrightarrow \mathrm{Br}(L_1/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(L_2/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L_2/L_1)$$
   It is the Inf-Res exact sequence. This can be proved by using Hilbert 90.
2. $\mathrm{Br}(L/K) = \mathrm{Ker}(\mathrm{Br}(K) \to \mathrm{Br}(L))$.
   (This follows by replacing L_2 by $\overline{K}$ in the exact sequence in (1)).
3. $\mathrm{Br}(K)$ classifies central simple algebras over K.
   Wedderburn's Theorem: Finite dimensional simple algebras over K are always of the form $M_n(D)$, where D is a division K-algebra.
   We say $A \sim B$ if $A \otimes_K M_n(K) \cong B \otimes_K M_m(K)$. For example: $D \sim M_n(D)$.

Example 13.2.

(1) $K = \overline{K}$, then $\mathrm{Br}(K) = 0$.

(2) $K = \mathbb{F}_q$ is a finite field. Then $\mathrm{Br}(K) = 0$.

(3) $K = \mathbb{R}$. $\mathrm{Br}(\mathbb{R}) = \{\pm 1\}$. We will construct an isomorphism:
$$\mathrm{inv} : \mathrm{Br}(\mathbb{R}) \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}, \quad -1 \longmapsto \frac{1}{2}, \quad 1 \longmapsto 0$$
Remark: In the sense of central simple algebras, $+1$ corresponds to $\mathbb{R}$, -1 corresponds to the Hamiltonian quaternions $\mathbb{H}$.

(4) We will construct an isomorphism $\mathrm{Br}(K) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z}$ for a p-adic field K.

(5) Let K be a p-adic field. Then $\mathrm{Br}(K^{\mathrm{ur}}) = 0$.

(6) Let K be a number field. Then we have the exact sequence:

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v \in V_K} \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Proof of (2). For all $n \in \mathbb{N}^*$, $\mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) = H^2(\mathbb{F}_{q^n}/\mathbb{F}_q, \mathbb{F}_{q^n}^*)$, where $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic, $\mathbb{F}_{q^n}^*$ is finite group. By **Theorem 12.2 (2)**, $h(\mathbb{F}_{q^n}^*) = 1$, and we note that $H^2(\mathbb{F}_{q^n}/\mathbb{F}_q, \mathbb{F}_{q^n}^*) = \hat{H}^0(\mathbb{F}_{q^n}/\mathbb{F}_q, \mathbb{F}_{q^n}^*)$, $H^1(\mathbb{F}_{q^n}/\mathbb{F}_q, \mathbb{F}_{q^n}^*) = 0$. So $\mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) = 0$ for all n. So $\mathrm{Br}(\mathbb{F}_q) = 0$. □

Proof of (3).

$$\begin{aligned}\mathrm{Br}(\mathbb{R}) &= H^2(\mathbb{C}/\mathbb{R}, \mathbb{C}^*) \cong \hat{H}^0(\mathbb{C}/\mathbb{R}, \mathbb{C}^*) \\ &= \mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) \cong \{\pm 1\}.\end{aligned}$$

□

13.2 Computation of Brauer group for p-adic fields

From now on, let K be a p-adic field.

Goal: Our goal is to prove the following theorem.

Theorem 13.2.

1. There is an isomorphism $\mathrm{inv} : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$.
2. Let L/K be a finite extension. The following diagrams commute:

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle \cdot[L:K]} \\ \mathrm{Br}(L) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \end{array} \qquad \begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ \uparrow{\scriptstyle \mathrm{Cor}} & & \| \\ \mathrm{Br}(L) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Remark: The second diagram follows from the first one by $\mathrm{Cor} \circ \mathrm{Res} = [L : K]$.

Strategy of proof of Theorem 13.2.

- **Step 1**: $\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ with desired properties.

- **Step 2**: L/K is a finite extension. Then the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{Res}} & & \Big\downarrow{\scriptstyle \cdot[L:K]} \\ \mathrm{Br}(L^{\mathrm{ur}}/L) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

- **Step 3**: Let L/K be a finite extension. Then $|\mathrm{Br}(L/K)| = [L:K]$.
- **Step 4**: $\mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow[\cong]{\mathrm{Inf}} \mathrm{Br}(K)$ is an isomorphism.

□

We first prove a lemma for Step 1:

Lemma 13.2. Let L/K be a finite unramified extension. Then

$$\hat{H}^n(L/K, \mathcal{O}_L^*) = 0, \quad \forall n \in \mathbb{Z}$$

i.e. $\mathcal{O}_L^*$ is a cohomologically trivial $G := \mathrm{Gal}(L/K)$-module.

Proof of Lemma 13.2. $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$ is a cyclic group. It suffices to show $\hat{H}^0 = \hat{H}^1 = 0$.

Since $L^* \cong \mathcal{O}_L^* \times \mathbb{Z}$, because $H^n(G, -)$ is additive functor,

$$\hat{H}^1(L/K, \mathcal{O}_L^*) \cong \hat{H}^1(L/K, L^*) \oplus \hat{H}^1(L/K, \mathbb{Z}) = 0$$

by Hilbert 90 and $H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$ (since G is finite).

$$\hat{H}^0(L/K, \mathcal{O}_L^*) = \mathcal{O}_K^*/N_{L/K}(\mathcal{O}_L^*) = 0$$

This follows from **Homework 6.2**. □

Corollary 13.2. $H^n(K^{\mathrm{ur}}/K, \mathcal{O}_{K^{\mathrm{ur}}}^*) = 0, \quad \forall n > 0.$

Proof of Step 1 of Theorem 13.2. Consider the exact sequence $0 \longrightarrow \mathcal{O}_{K^{\mathrm{ur}}}^* \longrightarrow K^{\mathrm{ur}*} \xrightarrow{\mathrm{ord}} \mathbb{Z} \longrightarrow 0$ as $\hat{\mathbb{Z}} = G = \mathrm{Gal}(K^{\mathrm{ur}}/K)$-modules. We can get $\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ by:

$$\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow[\cong]{\mathrm{ord}} H^2(K^{\mathrm{ur}}/K, \mathbb{Z}) \xrightarrow[\cong]{\delta^{-1}} H^1(K^{\mathrm{ur}}/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

The first isomorphism follows from **Corollary 13.2**, the second isomorphism follows from the **Homework 10.1**. The last isomorphism follows from:

$$\begin{aligned} H^1(K^{\mathrm{ur}}/K, \mathbb{Q}/\mathbb{Z}) &= \mathrm{Hom}_{\mathrm{cont}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \\ &= \varinjlim_n \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \varinjlim \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z} \end{aligned}$$

maps $f \in \mathrm{Hom}_{\mathrm{cont}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ to $f(\mathrm{Frob}) \in \mathbb{Q}/\mathbb{Z}$. □

Proof of Step 2 of Theorem 13.2. Let L/K be a finite extension, $L^{\mathrm{ur}} = L \cdot K^{\mathrm{ur}}$. We have $\mathrm{Gal}(L^{\mathrm{ur}}/L) \hookrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K)$. We have the following commutative diagram:

$$\begin{array}{ccccccccc} \mathrm{Br}(K^{\mathrm{ur}}/K) & = & H^2(K^{\mathrm{ur}}/K, K^{\mathrm{ur}*}) & \xrightarrow{\mathrm{ord}_K} & H^2(K^{\mathrm{ur}}/K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(K^{\mathrm{ur}}/K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e(L/K)\mathrm{Res}} & & \downarrow{\scriptstyle e(L/K)\mathrm{Res}} & & \downarrow{\scriptstyle \cdot[L:K]} \\ \mathrm{Br}(L^{\mathrm{ur}}/L) & = & H^2(L^{\mathrm{ur}}/L, L^{\mathrm{ur}*}) & \xrightarrow{\mathrm{ord}_L} & H^2(L^{\mathrm{ur}}/L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(L^{\mathrm{ur}}/L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Q}/\mathbb{Z} \end{array}$$

The identification of the last square is given by:

$$\begin{aligned} H^1(K^{\mathrm{ur}}/K, \mathbb{Q}/\mathbb{Z}) &\xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}, \quad f \longmapsto f(\mathrm{Frob}_K) \\ H^1(L^{\mathrm{ur}}/L, \mathbb{Q}/\mathbb{Z}) &\xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}, \quad f \longmapsto f(\mathrm{Frob}_L) \end{aligned}$$

We have $\mathrm{Frob}_L = \mathrm{Frob}_K^{f(L/K)}$. The vertical map is induced by $e(L/K)\mathrm{Res}$, and since $e(L/K)f(L/K) = [L:K]$, the diagram commutes. □

Corollary 13.3. Let $n \geq 1$. Let K_n/K be the unique unramified extension of degree n. Then we have a commutative diagram:

$$\begin{array}{ccc} \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow[\sim]{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{Inf}}\uparrow & & \uparrow \\ \mathrm{Br}(K_n/K) & \xrightarrow[\sim]{\mathrm{inv}} & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \end{array}$$

Proof of Corollary 13.3. Consider the exact sequence:

$$0 \longrightarrow \mathrm{Br}(K_n/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(K^{\mathrm{ur}}/K_n)$$

Using the isomorphism inv from Theorem A and the property of Restriction (which corresponds to multiplication by n on $\mathbb{Q}/\mathbb{Z}$ in the unramified case), we have:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Br}(K_n/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(K^{\mathrm{ur}}/K_n) \\ & & \downarrow{\scriptstyle \exists!\cong} & & \downarrow{\scriptstyle \cong}\,\mathrm{inv} & & \downarrow{\scriptstyle \cong}\,\mathrm{inv} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

This implies $\mathrm{Br}(K_n/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

We then prove a lemma for Step 3:

Lemma 13.3. Let L/K be a finite Galois extension. $G = \mathrm{Gal}(L/K)$. Then there exists an open subgroup V of $\mathcal{O}_L^*$ stable under G such that $H^n(G, V) = 0$ for all $n > 0$.

Proof of Lemma 13.3. **Claim:** There exists $\tilde{V} \subseteq \mathcal{O}_L$ open subgroup stable under G such that $H^n(G, \tilde{V}) = 0$ for all $n > 0$.

By the normal basis theorem, there exists $\beta \in \mathcal{O}_L$ such that $\{g\beta\}_{g\in G}$ form a K-basis of L. Let $\tilde{V} = \bigoplus_{g\in G} \mathcal{O}_K g\beta \cong \mathcal{O}_K[G] \cong \mathrm{ind}_1^G \mathcal{O}_K$. The claim follows.

The exponential map $\exp(x) = 1 + x + \frac{x^2}{2} + \dots$ converges when $\mathrm{ord}(x) \gg 0$. It defines an isomorphism of an open neighborhood of 0 in L and 1 in L^*. And it commutes with the G-action.

Then consider $V = \exp(\pi_K^m \tilde{V})$ for $m \gg 0$. □

Proof of Step 3 of Theorem 13.2. Denote $n := [L : K]$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Br}(L/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \mathrm{Inf}} & & \uparrow{\scriptstyle \mathrm{Inf}} & & \\ 0 & \longrightarrow & \mathrm{Br}(K_n/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L^{\mathrm{ur}}/L) & \dashrightarrow & 0 \\ & & \downarrow{\scriptstyle \cong}\,\mathrm{inv} & & \downarrow{\scriptstyle \cong}\,\mathrm{inv} & & \downarrow{\scriptstyle \cong}\,\mathrm{inv} & & \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

Logic Chain of the diagram:

1. **Row 3 is Exact**: This is the standard exact sequence of coefficients.

2. **Row 3 ⇒ Row 2**: Since all vertical maps between Row 2 and Row 3 are isomorphisms (inv), and Row 3 is exact, and the solid squares between Row 3 and Row 2 commute (respectively comes from **Corollary 13.3** and **Step 2**), **Row 2 must be exact**.

3. **Commutativity**: The solid square between Row 2 and Row 1 commutes (properties of Inflation and Restriction).

4. **Induced Map**:

   - Row 2 is exact.
   - Row 1 is exact. (by the previous **Remark**).
   - It is easy to construct the unique induced homomorphism $\varphi : \mathrm{Br}(K_n/K) \to \mathrm{Br}(L/K)$.

5. **Injectivity**: Since the middle vertical map $\mathrm{Inf} : \mathrm{Br}(K^{\mathrm{ur}}/K) \to \mathrm{Br}(K)$ is injective, the induced map φ is **injective**.

So $|\mathrm{Br}(L/K)| \geqslant |\mathrm{Br}(K_n/K)| = n$. Now we are going to show $|\mathrm{Br}(L/K)| \leqslant n$.

Case 1. L/K cyclic. anchor text

Claim: $h(\mathcal{O}_L^*) = 1$, $h(L^*) = [L : K]$.

By **Lemma 13.3**, there exists $V \subseteq \mathcal{O}_L^*$ open subgroup stable under $G = \mathrm{Gal}(L/K)$ such that $H^n(G, V) = 0$ for all $n > 0$. So $h(V) = 1$. Consider the following G-module exact sequence:

$$0 \longrightarrow V \longrightarrow \mathcal{O}_L^* \longrightarrow \underbrace{\mathcal{O}_L^*/V}_{\text{finite}} \longrightarrow 0$$

(finiteness comes from the compactness of $\mathcal{O}_L^*$) So $h(\mathcal{O}_L^*) = h(\mathcal{O}_L^*/V) \cdot h(V) = 1 \cdot 1 = 1$. Then consider the following G-module exact sequence:

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

So $h(L^*) = h(\mathbb{Z}) \cdot h(\mathcal{O}_L^*) = n \cdot 1 = n$. The claim is proved.

Because L/K cyclic and Hilbert 90:

$$|\mathrm{Br}(L/K)| = |H^2(G, L^*)| = |\hat{H}^0(G, L^*)| = h(L^*) \cdot |H^1(G, L^*)| = n \cdot 1 = n$$

We've done case 1.

Case 2. General.

We prove by induction on $[L : K]$. We need the following fact.

Fact: $G = \mathrm{Gal}(L/K)$ is solvable for L/K finite extension.

If we can find a proper intermediate field $K \subsetneq K' \subsetneq L$ with K'/K Galois extension. Then by the exact sequence given in the previous **Remark**:

$$0 \longrightarrow \mathrm{Br}(K'/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(L/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L/K') \longrightarrow 0$$

We have: $|\mathrm{Br}(L/K)| = |\mathrm{Br}(K'/K)| \cdot |\mathrm{Br}(L/K')| \leqslant [K' : K] \cdot [L : K'] = [L : K]$.

If we can not find such an intermediate field. By the fact, G is a simple abelian group, which is cyclic group. Then reduce to case 1. □

Proof of Step 4 of Theorem 13.2. From the process in proof of Step 3, we construct isomorphism $\varphi : \mathrm{Br}(K_n/K) \to \mathrm{Br}(L/K)$. We can consider this map as the transition map. Then:

$$\mathrm{Br}(K) = \varinjlim_{L/K \text{ Galois}} \mathrm{Br}(L/K) \cong \varinjlim_{n} \mathrm{Br}(K_n/K) \cong \mathrm{Br}(K^{\mathrm{ur}}/K)$$

Need details on the commutativity of the transition maps. Main idea is to consider image on $\mathbb{Q}/\mathbb{Z}$. □

We list two important conclusions in the proof of **Theorem 13.2**:

Theorem 13.3. $\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ with desired properties in **Theorem 13.2**.

Proposition 13.2. Let L/K be a finite extension. Then $|\mathrm{Br}(L/K)| = [L : K]$.

13.3 Local Artin map

Let L/K be a finite Galois extension, $n = [L : K]$.

$$\begin{aligned} \mathrm{inv} : \mathrm{Br}(L/K) &\xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ u_{L/K} &\longmapsto \frac{1}{n} \end{aligned}$$

Definition 13.6. $u_{L/K}$ is called the **fundamental class** of L/K.

Now we try to apply **Tate-Nakayama Theorem** to our situation. $G = \mathrm{Gal}(L/K)$,

$A = L^*$, $a = u_{L/K}$. Let $K^p = L^{G_p}$.

$$\begin{array}{c} L \\ | \\ K^p = L^{G_p} \\ | \\ K \end{array}$$

We verify the assumptions in **Tate-Nakayama Theorem**:

(a) $H^1(G_p, A) = H^1(L/K^p, L^*) = 0$ by Hilbert 90.

(b) $H^2(G_p, A) = \mathrm{Br}(L/K^p)$.

From the commutative diagram we know:

$$\begin{array}{ccc} \mathrm{Br}(L/K) & \xrightarrow{\sim} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \cdot[K_p:K]} \\ \mathrm{Br}(L/K_p) & \xrightarrow{\sim} & \frac{1}{[L:K_p]}\mathbb{Z}/\mathbb{Z} \end{array}$$

- $\mathrm{Br}(L/K^p)$ is a cyclic group of order $[L : K^p] = |G_p|$ generated by u_{L/K^p}.
- $\downarrow \circ \leftarrow$ maps $u_{L/K}$ to $\frac{1}{[L:K^p]}$, so $\mathrm{Res}\, u_{L/K} = u_{L/K^p}$.

So (b) is verified.

Remark: When $K \subseteq M \subseteq L$ are Galois extensions, then $\mathrm{Res}\, u_{L/K} = u_{L/M}$.

By applying **Tate-Nakayama theorem**, we get an isomorphism:

$$-\cup u_{L/K}: \quad \begin{array}{ccc} \hat{H}^{-2}(G, \mathbb{Z}) & \xrightarrow{\cong} & \hat{H}^0(G, L^*) \\ \downarrow{\scriptstyle \cong} & & \| \\ G^{\mathrm{ab}} & & K^*/N_{L/K}(L^*) \end{array}$$

Definition 13.7. The **local Artin map** $\psi_{L/K} : K^* \longrightarrow K^*/N_{L/K}(L^*) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}$.

Remark: $\psi_{L/K}$ exists for all L/K finite Galois extensions.

Theorem 13.4. $\ker \psi_{L/K} = N_{L/K}(L^*)$

There exists an explicit way to characterize $\psi_{L/K}$ for L/K abelian. See the following proposition.

Proposition 13.3. Let L/K be a finite abelian extension of p-adic fields. Let $G = \mathrm{Gal}(L/K)$. For all $\chi : G \to \mathbb{Q}/\mathbb{Z}$ character (i.e. $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$), for all $a \in K^*$:

$$\underbrace{\chi(\psi_{L/K}(a))}_{\in \mathbb{Q}/\mathbb{Z}} = \mathrm{inv}_K\Big(\underbrace{a}_{\in \hat{H}^0(G, L^*)} \cup \underbrace{\delta\chi}_{\in \hat{H}^2(G,\mathbb{Z})} \Big)$$

We will prove it in the next lecture.

14 2025.12.7

Review:

- Let L/K be a finite extension of a p-adic field. The invariant map is given by:

$$\begin{aligned} \mathrm{inv}_{L/K} : H^2(L/K, L^*) = \mathrm{Br}(L/K) &\xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ u_{L/K} &\longmapsto \frac{1}{n} \end{aligned}$$

  Notation: If no other fields are in question, we simply write inv_K instead of $\mathrm{inv}_{L/K}$.

- By **Tate-Nakayama Theorem** We have the isomorphism induced by the cup product with the fundamental class:

$$\begin{aligned} - \cup u_{L/K} : \hat{H}^{-2}(L/K, \mathbb{Z}) &\xrightarrow{\sim} \hat{H}^0(L/K, L^*) \\ \mathrm{Gal}(L/K)^{\mathrm{ab}} &\cong K^*/N_{L/K}(L^*) \end{aligned}$$

- The **Local Artin map** is defined as:

$$\psi_{L/K} : K^* \longrightarrow \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

  with kernel $N_{L/K}(L^*)$.

Proposition 14.1. Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Let $\chi : G \longrightarrow \mathbb{Q}/\mathbb{Z}$ be a character (i.e., $\chi \in H^1(L/K, \mathbb{Q}/\mathbb{Z})$). Then for all $a \in K^*$,

$$\chi(\psi_{L/K}(a)) = \mathrm{inv}_{L/K}(\bar{a} \cup \delta\chi) \in \mathbb{Q}/\mathbb{Z}.$$

Proof. Let $s = \psi_{L/K}(a) \in G^{\mathrm{ab}} = \hat{H}^{-2}(L/K, \mathbb{Z})$. From the definition of the Artin map via Tate-Nakayama, we have:

$$\bar{a} = s \cup u_{L/K} \in \hat{H}^0(L/K, L^*).$$

For the LHS, let $|G| = n$. We have $\chi(s) = \frac{r}{n} \in \mathbb{Q}/\mathbb{Z}$.

Now we compute the term inside the invariant on the RHS:

$$\begin{aligned}\bar{a} \cup \delta\chi &= s \cup u_{L/K} \cup \delta\chi \\ &= u_{L/K} \cup (s \cup \delta\chi) \quad \text{(Since the degrees are even, the sign } (-1) \text{ does not appear)} \\ &= u_{L/K} \cup (\delta(s \cup \chi)) \quad \text{(Since the degrees are even, the sign } (-1) \text{ does not appear)} \\ &= u_{L/K} \cup \delta(\chi(s)) \quad \text{(by } \textbf{Homework 11.5}\text{)}.\end{aligned}$$

Where $\chi(s)$ is considered as an element in $\hat{H}^{-1}(L/K, \mathbb{Q}/\mathbb{Z})$. Notice that:

$$\begin{aligned}\delta : \hat{H}^{-1}(L/K, \mathbb{Q}/\mathbb{Z}) &\longrightarrow \hat{H}^0(L/K, \mathbb{Z}) \\ \frac{1}{n}\mathbb{Z}/\mathbb{Z} &\longrightarrow \operatorname{coker}(\mathbb{Z} \xrightarrow{n} \mathbb{Z}) \\ \frac{r}{n} &\longmapsto r.\end{aligned}$$

δ is actually multiplying by n. So:

$$\bar{a} \cup \delta\chi = u_{L/K} \cup \delta(\chi(s)) = u_{L/K} \cup r = r u_{L/K} \in \hat{H}^2(L/K, L^*).$$

Therefore,

$$\text{RHS} = \operatorname{inv}_{L/K}(\bar{a} \cup \delta\chi) = \operatorname{inv}_{L/K}(r u_{L/K}) = \frac{r}{n} = \text{LHS}.$$

□

Before giving the following corollary, we state an exercise about profinite group.

Exercise 14.1. Let G be a profinite group and $G' \subseteq G$ a subgroup. Then G' is dense in G if and only if the map $G' \longrightarrow G/H$ is surjective for all open normal subgroups $H \trianglelefteq G$.

Corollary 14.1. Let $M \supseteq L \supseteq K$ be finite Galois extensions. We have a commutative diagram:

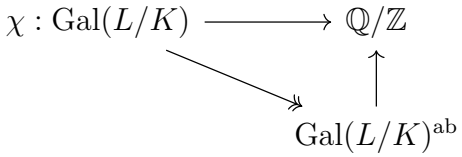
$$\begin{array}{ccccc} & & K^*/N_{M/K}(M^*) & \xrightarrow{\psi_{M/K}} & \operatorname{Gal}(M/K)^{\mathrm{ab}} \\ & \nearrow & \downarrow & & \downarrow \\ K^* & \longrightarrow & K^*/N_{L/K}(L^*) & \xrightarrow[\psi_{L/K}]{} & \operatorname{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

Passing to the limit, we have the local Artin map

$$\psi_K : K^* \longrightarrow \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$$

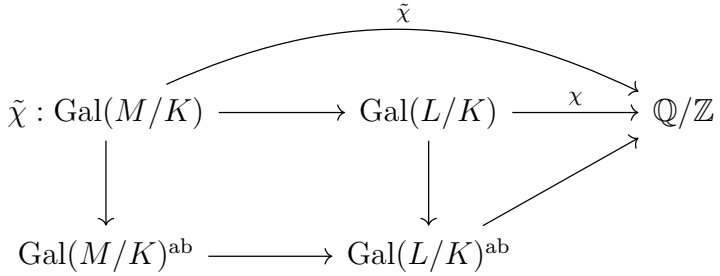
with dense image.

Proof of Corollary. Let $\chi \in H^1(L/K, \mathbb{Q}/\mathbb{Z})$ be a character. We have the diagram:



i.e. χ factors through $\mathrm{Gal}(L/K)^{\mathrm{ab}}$.

We define $\tilde{\chi}$ via the following commutative diagram:



Since the characters separate points in the abelianization, two elements $g, h \in \mathrm{Gal}(L/K)^{\mathrm{ab}}$ are equal if and only if $\chi(g) = \chi(h)$ for all characters $\chi \in H^1(L/K, \mathbb{Q}/\mathbb{Z})$. So in order to prove the diagram commutes, our **Goal** is to prove:

$$\chi \circ \psi_{L/K}(a) = \tilde{\chi} \circ \psi_{M/K}(a)$$

for all $a \in K^*$.

Notice that in the inflation map on cohomology:

$$\begin{aligned} \mathrm{Inf} : \hat{H}^1(L/K, \mathbb{Q}/\mathbb{Z}) &\longrightarrow H^1(M/K, \mathbb{Q}/\mathbb{Z}) \\ \chi &\longmapsto \tilde{\chi} \end{aligned}$$

By **Proposition 14.1**, we have:

$$\begin{aligned} \chi \circ \psi_{L/K}(a) &= \mathrm{inv}_{L/K}(\bar{a} \cup \delta\chi) \\ \tilde{\chi} \circ \psi_{M/K}(a) &= \mathrm{inv}_{M/K}(\bar{a} \cup \delta\tilde{\chi}) \end{aligned}$$

So it suffices to show:

$$\mathrm{inv}_{L/K}(\bar{a} \cup \delta\chi) = \mathrm{inv}_{M/K}(\bar{a} \cup \delta\tilde{\chi})$$

We have the commutative diagram for the invariant maps:

$$\begin{array}{ccc} \mathrm{Br}(L/K) & & \\ {\scriptstyle \mathrm{Inf}}\downarrow & \searrow^{\mathrm{inv}} & \\ \mathrm{Br}(M/K) & \xrightarrow[\mathrm{inv}]{} & \mathbb{Q}/\mathbb{Z} \end{array}$$

So it suffices to show that $\mathrm{Inf}(\overline{a} \cup \delta\chi) = \overline{a} \cup \delta\tilde{\chi}$ in $\mathrm{Br}(M/K)$. This holds because $\tilde{\chi} = \mathrm{Inf}(\chi)$ and $\mathrm{Inf}(\overline{a}) = \overline{a}$ and **Proposition 12.1(4)** and functoriality of δ. □

Proposition 14.2.

1. If L/K is a finite unramified extension, then $\psi_{L/K}(\pi_K) = \mathrm{Frob}_K$.
2. (Functoriality) We have the following commutative diagrams:

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_L} & \mathrm{Gal}(\bar{L}/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow{\psi_K} & \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} L^* & \xrightarrow{\psi_L} & \mathrm{Gal}(\bar{L}/L)^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^* & \xrightarrow{\psi_K} & \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}} \end{array}$$

Proof of (1). It suffices to show that:

$$\chi(\psi_{L/K}(\pi_K)) = \chi(\mathrm{Frob}_K) \quad \forall \chi \in \hat{H}^1(L/K, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}).$$

We know that $\chi(\psi_{L/K}(\pi_K)) = \mathrm{inv}_K(\bar{\pi}_K \cup \delta\chi)$. Consider the definition of inv_K:

$$\mathrm{inv}_K : H^2(L/K, L^*) \xrightarrow{\mathrm{ord}_L} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

$$f \longmapsto f(\mathrm{Frob})$$

And the following commutative diagram:

$$\begin{array}{ccc} H^2(L/K, L^*) & \xrightarrow{\qquad\mathrm{ord}_L\qquad} & H^2(L/K, \mathbb{Z}) \\ \cup\uparrow & & \cup\uparrow \\ \hat{H}^0(L/K, L^*) \times H^2(L/K, \mathbb{Z}) & \xrightarrow{\mathrm{ord}_L} & \hat{H}^0(L/K, \mathbb{Z}) \times H^2(L/K, \mathbb{Z}) \end{array}$$

So:

$$\begin{aligned}\chi(\psi_{L/K}(\pi_K)) &= \mathrm{inv}_K(\bar{\pi}_K \cup \delta\chi) \\ &= (\delta^{-1} \circ \mathrm{ord}_L(\bar{\pi}_K \cup \delta\chi))(\mathrm{Frob}) \\ &= (\delta^{-1}(\mathrm{ord}_L(\bar{\pi}_K) \cup \delta\chi))(\mathrm{Frob}) \\ &= (\delta^{-1}(1 \cup \delta\chi))(\mathrm{Frob}) = (\delta^{-1}(\delta\chi))(\mathrm{Frob}) = \chi(\mathrm{Frob})\end{aligned}$$

□

Proof of (2). It suffices to show that for all $M \supseteq L \supseteq K$ such that M/K is a finite Galois extension, we have:

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_{M/L}} & \mathrm{Gal}(M/L)^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ K^* & \xrightarrow{\psi_{M/K}} & \mathrm{Gal}(M/K)^{\mathrm{ab}} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} L^* & \xrightarrow{\psi_{M/L}} & \mathrm{Gal}(M/L)^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^* & \xrightarrow{\psi_{M/K}} & \mathrm{Gal}(M/K)^{\mathrm{ab}} \end{array}$$

The local Artin map is essentially the cup product. It is equivalent to show the commutativity of the following diagrams:

$$\begin{array}{ccc} \hat{H}^0(M/L, M^*) & \xleftarrow[\sim]{-\cup u_{M/L}} & \hat{H}^{-2}(M/L, \mathbb{Z}) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ \hat{H}^0(M/K, M^*) & \xleftarrow[\sim]{-\cup u_{M/K}} & \hat{H}^{-2}(M/K, \mathbb{Z}) \end{array} \qquad \begin{array}{ccc} \hat{H}^0(M/L, M^*) & \longleftarrow & \hat{H}^{-2}(M/L, \mathbb{Z}) \\ {\scriptstyle \mathrm{Res}}\uparrow & & \uparrow{\scriptstyle \mathrm{Res}} \\ \hat{H}^0(M/K, M^*) & \longleftarrow & \hat{H}^{-2}(M/K, \mathbb{Z}) \end{array}$$

We want to show:

$$\begin{aligned}\mathrm{Cor}(\bar{b} \cup u_{M/L}) &= \mathrm{Cor}(\bar{b}) \cup u_{M/K} \\ \mathrm{Res}(\bar{a} \cup u_{M/K}) &= \mathrm{Res}(\bar{a}) \cup u_{M/L}\end{aligned}$$

where we used the fact that $u_{M/L} = \mathrm{Res}(u_{M/K})$ and **Proposition 12.1(3)(5)**. □

14.1 Existence Theorem and Hilbert Symbol

Theorem 14.1 (**Existence Theorem**)**.** Any open subgroup of K^* of finite index is of the form $N_{L/K}(L^*)$ for some finite extension L/K.

Before proving the theorem, we state the following propositions:

Proposition 14.3.

1. If L/K is a finite abelian extension, then $N_{L/K}(L^*) \subseteq K^*$ is open and of finite index.
2. Let $U \subseteq K^*$ be a subgroup of K^*. Assume that U contains a subgroup $V = N_{E/K}(E^*)$ with E/K being a finite abelian extension. Then U itself is also of this form.

Proposition 14.4 (**Norm Limitation Theorem**)**.** Let E/K be a finite extension. Let L/K be the maximal abelian extension of K contained in E. Then $N_{E/K}(E^*) = N_{L/K}(L^*)$.

Proposition 14.5. Suppose $K \supseteq \mu_n$ (where $n \geq 2$). Then $K^{*n} = N_{L/K}(L^*)$ for some finite abelian extension L/K.

Proof of Theorem (assuming the propositions above). Let $U \subseteq K^*$ be an open subgroup of finite index. Suppose $[K^* : U] = n$. Then $K^{*n} \subseteq U$. Let $F = K(\zeta_n)$. Apply **Proposition 14.5** to F. Then $F^{*n} = N_{E/F}(E^*)$ for some finite abelian extension E/F. We have:

$$U \supseteq K^{*n} \supseteq N_{F/K}(F^{*n}) = N_{F/K}(N_{E/F}(E^*)) = N_{E/K}(E^*).$$

Apply **Proposition 14.4** to the extension E/K. Let L be the maximal abelian extension of K contained in E. Then $N_{E/K}(E^*) = N_{L/K}(L^*)$. Thus $U \supseteq N_{L/K}(L^*)$. By **Proposition 14.3(2)**, U is of the form $N_{M/K}(M^*)$ for some finite abelian extension M/K. □

Proof of Proposition 14.3(1). By Artin Reciprocity, we have $[K^* : N_{L/K}(L^*)] = |\mathrm{Gal}(L/K)|$. This implies that $N_{L/K}(L^*)$ is of finite index in K^*. It remains to show that $N_{L/K}(L^*)$ is a closed subgroup. We have the following diagram:

$$\begin{array}{ccc} L^* & \xrightarrow{\cong} & \mathcal{O}_L^* \times \mathbb{Z} \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N \times f(L/K)} \\ K^* & \xrightarrow{\cong} & \mathcal{O}_K^* \times \mathbb{Z} \end{array}$$

The map $\mathcal{O}_L^* \longrightarrow \mathcal{O}_K^*$ has a closed image because $\mathcal{O}_L^*$ is profinite, which implies it is compact. Since the map is continuous and the target is Hausdorff, the image is compact and therefore closed. The image of $N_{L/K}$ in K^* corresponds to $N_{L/K}(\mathcal{O}_L^*) \times f(L/K)\mathbb{Z}$, which is closed in $\mathcal{O}_K^* \times \mathbb{Z}$. □

Proof of Proposition 14.3(2). Let $K^* \supseteq U \supseteq V$, where $V = N_{E/K}(E^*)$. We have

$$\psi_{E/K} : K^*/V = K^*/N_{E/K}(E^*) \longrightarrow \mathrm{Gal}(E/K)$$

Let L be the intermediate field such that $\psi_{E/K}(U/V) = \mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/K)$. Then by **Corollary 14.1**:

$$\begin{array}{ccc} K^*/N_{E/K}(E^*) & \xrightarrow[\sim]{\psi_{E/K}} & \mathrm{Gal}(E/K) \\ \Big\downarrow{\scriptstyle \text{quotient}} & & \Big\downarrow{\scriptstyle \text{Restriction on } L} \\ K^*/N_{L/K}(L^*) & \xrightarrow[\sim]{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

It is easy to deduce $U = N_{L/K}(L^*)$. □

Proof of Proposition 14.4. **Case 1:** E/K is a finite Galois extension. We have the identification $\mathrm{Gal}(E/K)^{\mathrm{ab}} = \mathrm{Gal}(L/K)$, where L is the maximal abelian extension of K contained in E. Consider the commutative diagram:

$$\begin{array}{ccc} K^*/N_{E/K}(E^*) & \xrightarrow[\sim]{\psi_{E/K}} & \mathrm{Gal}(E/K)^{\mathrm{ab}} \\ \Big\downarrow & & \Big\| \\ K^*/N_{L/K}(L^*) & \xrightarrow[\sim]{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Since the horizontal maps are isomorphisms and the right vertical map is the identity, the left vertical map must be an isomorphism. Therefore $N_{E/K}(E^*) = N_{L/K}(L^*)$.

Case 2: General case.

Let M/K be the Galois closure of the finite extension E/K. Let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/E)$. Let $\mathrm{Gal}(M/L)$ be the smallest subgroup of G among subgroups $G' \supseteq H$ such that G/G' is abelian (i.e., $G' \supseteq G^{\mathrm{der}}$). Then $\mathrm{Gal}(M/L) = H \cdot G^{\mathrm{der}}$.

We want to show $N_{E/K}(E^*) = N_{L/K}(L^*)$.

"$\subseteq$": This is obvious since $L \subseteq E$.

"$\supseteq$": Let $a \in N_{L/K}(L^*)$. Consider the following commutative diagram based on **Corol-**

lary 14.1 and **norm functoriality**:

$$\begin{array}{ccc} E^* & \xrightarrow{\psi_{M/E}} & H^{\mathrm{ab}} \\ {\scriptstyle N_{E/K}}\downarrow & & \downarrow{\scriptstyle f} \\ K^* & \xrightarrow{\psi_{M/K}} & G^{\mathrm{ab}} \\ \| & & \downarrow \\ K^* & \xrightarrow{\psi_{L/K}} \operatorname{coker} f = G/(G^{\mathrm{der}} \cdot H) = G/G' = \mathrm{Gal}(L/K) & \end{array}$$

From the diagram, since $a \in N_{L/K}(L^*)$, its image in $\mathrm{Gal}(L/K)$ is trivial. This implies that $\psi_{M/K}(a)$ lies in the image of f. Since $\psi_{M/E}$ is surjective, there exists $b \in E^*$ such that

$$\psi_{M/K}(a) = \psi_{M/K}(N_{E/K}(b)).$$

We know that the kernel of the Artin map is the norm group:

$$\ker \psi_{M/K} = N_{M/K}(M^*).$$

Therefore,

$$\begin{aligned} a &= N_{E/K}(b) \cdot N_{M/K}(c) \quad \text{for some } c \in M^* \\ &= N_{E/K}(b \cdot N_{M/E}(c)). \end{aligned}$$

Since $b \cdot N_{M/E}(c) \in E^*$, we conclude that $a \in N_{E/K}(E^*)$. □

To prove Proposition 14.5, we need to introduce Hilbert Symbol.

Assume $K \supseteq \mu_n$ with $n \geq 2$. For any $b \in K^*$, let $K(\sqrt[n]{b})/K$ be a finite Galois extension.

Definition 14.1. The **Hilbert symbol** is a map

$$(-,-)_n := \left(\frac{-,-}{K}\right)_n : K^* \times K^* \longrightarrow \mu_n \subseteq K$$

defined by

$$(a,b) = \frac{\psi_{K(\sqrt[n]{b})/K}(a)(\sqrt[n]{b})}{\sqrt[n]{b}} \in \mu_n.$$

Remark: This definition does not depend on the choice of $\sqrt[n]{b}$.

Proposition 14.6. For all $a, b, a_1, a_2, b_1, b_2 \in K^*$:

1. $(a_1a_2, b) = (a_1, b) \cdot (a_2, b)$.
2. $(a, b_1b_2) = (a, b_1) \cdot (a, b_2)$.
3. $(a, b) = 1 \iff a \in N_{K(\sqrt[n]{b})/K}(K(\sqrt[n]{b})^*)$.
4. $(a, 1-a) = 1 = (a, -a)$.
5. $(a, b) = (b, a)^{-1}$.
6. $(a, b) = 1$ for all $a \in K^* \iff b \in (K^*)^n$.
7. $(a, b) = 1$ for all $b \in K^* \iff a \in (K^*)^n$.

Corollary 14.2. The map

$$(\cdot, \cdot)_n : K^*/(K^*)^n \times K^*/(K^*)^n \longrightarrow \mu_n$$

is a bilinear, non-degenerate form.

Remark: For the extension $\mathbb{C}/\mathbb{R}$:

$$\psi_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

where $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) = \mathbb{R}_{>0}$.

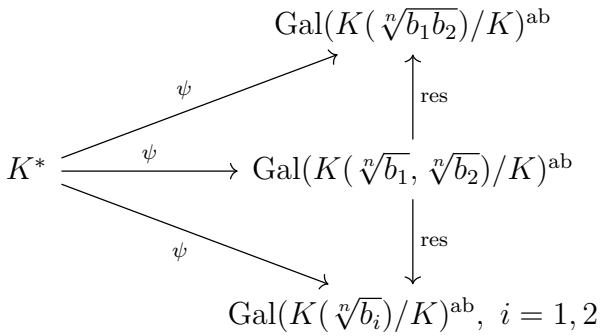
$$\left(\frac{a, b}{\mathbb{R}}\right)_2 = \frac{\psi_{\mathbb{R}(\sqrt{b})/\mathbb{R}}(a)(\sqrt{b})}{\sqrt{b}} = \begin{cases} -1 & \text{if } a < 0 \text{ and } b < 0 \\ 1 & \text{otherwise} \end{cases}$$

$$\implies \left(\frac{-, -}{\mathbb{R}}\right)_2 : \mathbb{R}^*/\mathbb{R}_{>0} \times \mathbb{R}^*/\mathbb{R}_{>0} \longrightarrow \{\pm 1\} \quad \text{satisfy the same properties.} \quad \square$$

Proof of Proposition 14.6.

1. $\psi_{K(\sqrt[n]{b})/K}$ is a group homomorphism.

2. Consider the diagram:



We can use $\psi_{K(\sqrt[n]{b_1}, \sqrt[n]{b_2})/K}$ to do the computation.

3.

$$\begin{aligned}(a, b) = 1 &\iff \psi_{K(\sqrt[n]{b})/K}(a) = 1 \\ &\iff a \in \ker \psi_{K(\sqrt[n]{b})/K} = N_{K(\sqrt[n]{b})/K}(K(\sqrt[n]{b})^*)\end{aligned}$$

4. By (3), it suffices to show $1 - a, -a \in N_{K(\sqrt[n]{a})/K}(K(\sqrt[n]{a})^*)$. (For the original problem, just note that we can replace $a \to 1 - a$, $a \to -a$).

   Consider the map:

$$\mathrm{Gal}(K(\sqrt[n]{a})/K) \hookrightarrow \mu_n \simeq \mathbb{Z}/n\mathbb{Z}$$

$$\sigma \longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

   It is a group homomorphism because $K \subseteq \mu_n$. Suppose its image is $m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ where $d|n$. Then $\mathrm{Gal}(K(\sqrt[n]{a})/K) \cong \mathbb{Z}/d\mathbb{Z}$.

   Let σ be a generator:

$$\sigma : \sqrt[n]{a} \longmapsto \zeta_n^m \sqrt[n]{a}$$

   Then for all $x \in K$:

$$x^n - a = \prod_{j=0}^{n-1}(x - \zeta_n^j \sqrt[n]{a}) = \prod_{j=0}^{m-1}\prod_{i=0}^{d-1}(x - \zeta_n^{mi}\zeta_n^j \sqrt[n]{a}) = N_{K(\sqrt[n]{a})/K}\left(\prod_{j=0}^{d-1}(x - \zeta_n^j \sqrt[n]{a})\right)$$

   Take $x = 0, 1$, then $-a, 1 - a$ is a norm.

5. Want to show $(a,b)(b,a)=1$.

$$\begin{aligned}\text{By (4), LHS} &= (a,b)(a,-a)(b,a)(b,-b)\\ \text{By (1)} &= (a,-ab)(b,-ab)\\ \text{By (2)} &= (ab,-ab)\\ \text{By (4)} &= 1.\end{aligned}$$

6. For all $a\in K^*$, $(a,b)=1$. Then $\psi_{K(\sqrt[n]{b})/K}(a)=1$. This implies that the map $\psi_{K(\sqrt[n]{b})/K}: K^*\longrightarrow \mathrm{Gal}(K(\sqrt[n]{b})/K)$ is trivial. Since the map is surjective, we have $\mathrm{Gal}(K(\sqrt[n]{b})/K)=\{1\}$. Therefore $K(\sqrt[n]{b})=K$, $b\in K^{*n}$.

7. By (5) and (6).

□

Now we prove **Proposition 14.5**.

Proof of Proposition 14.5. Assume $K\supseteq\mu_n$. Let $G:=\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Claim: nG is an open subgroup of finite index.

We have the commutative diagram with three exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_K & \longrightarrow & G & \xrightarrow{\mathrm{pr}} & \mathrm{Gal}(K^{\mathrm{ur}}/K) & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle\cdot n} & & \downarrow{\scriptstyle\cdot n} & & \downarrow{\scriptstyle\cdot n} & & \\
0 & \longrightarrow & I_K & \longrightarrow & G & \xrightarrow{\mathrm{pr}} & \hat{\mathbb{Z}} & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & I_K/nI_K & \longrightarrow & G/nG & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0
\end{array}$$

To show G/nG is finite, it suffices to show I_K/nI_K is finite. By **Corollary 6.4**,

$$I_K\cong\mathcal{O}_K^*$$

So it suffices to show $\mathcal{O}_K^*/\mathcal{O}_K^{*n}$ is finite. By exponential map, there exists an homeomorphism of an open neighborhood $\tilde{V}$ of $0\in\mathcal{O}_K$ to an open neighborhood V of $1\in\mathcal{O}_K^*$. Suppose $n\pi_K^m\mathcal{O}_K\subseteq\pi_K^m\mathcal{O}_K\subseteq\tilde{V}$ are open neighborhoods of $0\in\mathcal{O}_K$, from the homeomorphism, $\exp(n\pi_K^m\mathcal{O}_K)$ is an open neighborhood of $1\in\mathcal{O}_K^*$. From the compactness of $\mathcal{O}_K^*$, $[\mathcal{O}_K^*:\exp(n\pi_K^m\mathcal{O}_K)]<\infty$. Also it is obvious that $\exp(n\pi_K^m\mathcal{O}_K)\subseteq\mathcal{O}_K^{*n}$. So $[\mathcal{O}_K^*:\mathcal{O}_K^{*n}]<\infty$.

Consider the map $G\xrightarrow{n}G$. Since G is profinite, the image nG is closed in G. A closed subgroup of finite index is open, so nG is open in G. The claim is proved.

Let $L = (K^{\mathrm{ab}})^{nG}$. Then L/K is a finite abelian extension with Galois group:

$$\mathrm{Gal}(L/K) \cong G/nG.$$

We want to show that $K^{*n} = \ker \psi_{L/K} (= N_{L/K}(L^*))$.

- "$\subseteq$": The Artin map is $\psi_{L/K} : K^* \longrightarrow \mathrm{Gal}(L/K) = G/nG$. Since the target group has exponent n, we have $K^{*n} \subseteq \ker \psi_{L/K}$.
- "$\supseteq$": **Claim:** $L \supseteq K(\sqrt[n]{b})$ for all $b \in K^*$.

  Consider the projection $G = \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow \mathrm{Gal}(K(\sqrt[n]{b})/K)$. The target group is cyclic of order dividing n. Thus, the map factors through the quotient $G/nG = \mathrm{Gal}(L/K)$.

$$\begin{array}{ccc} G = \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K(\sqrt[n]{b})/K) \\ \downarrow & \nearrow & \\ G/nG = \mathrm{Gal}(L/K) & & \end{array}$$

  The claim follows.

  Now, for any $a \in \ker \psi_{L/K}$, consider the commutative diagram:

$$\begin{array}{ccc} K^* & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \\ & \searrow^{\psi_{K(\sqrt[n]{b})/K}} & \downarrow \\ & & \mathrm{Gal}(K(\sqrt[n]{b})/K) \end{array}$$

  We have $a \in \ker \psi_{K(\sqrt[n]{b})/K}$ for all $b \in K^*$. From **Proposition 14.6(3)**, the Hilbert symbol $(a, b) = 1$ for all $b \in K^*$. Then from **Proposition 14.6(7)**, we conclude that $a \in K^{*n}$.

□

15 2025.12.11

VII. Proof of Global Class Field Theory

15.1 Cohomology of ideles

Let K be a number field. We have the embedding $\mathbb{A}_K \hookrightarrow \mathbb{A}_K \otimes_K L \cong \mathbb{A}_L$, where L/K is a finite extension.

Remark: From now on, suppose L/K is a finite Galois extension.

Let $G = \mathrm{Gal}(L/K)$. Then $\mathbb{A}_K = \mathbb{A}_L^G$ and $\mathbb{I}_K = \mathbb{A}_K^*$. In particular, we have

$$H^0(L/K, \mathbb{I}_L) = \mathbb{I}_K.$$

For any $v \in V_K$, we have the decomposition

$$L \otimes_K K_v = \prod_{w|v} L_w.$$

The group G acts on this structure.

Definition 15.1. For $w|v$, we define the **decomposition group** as:

$$G_w := \mathrm{Gal}(L_w/K_v) = \{\sigma \in G \mid \sigma(L_w) = L_w\}.$$

Then as G-modules, we have:

$$L \otimes_K K_v = \prod_{w|v} L_w = \mathrm{Ind}_{G_w}^G L_w.$$

Remark: Let $w|v$ and $w'|v$. Suppose $w' = \sigma w$ for some $\sigma \in G$. We have the isomorphism:

$$\begin{aligned} G_w &\xrightarrow{\sim} G_{w'} \\ \tau &\longmapsto \sigma\tau\sigma^{-1} \end{aligned}$$

and the map:

$$\begin{aligned} L_{w'} &\longrightarrow L_w \\ x &\longmapsto \sigma^{-1}x \end{aligned}$$

From **Homework 11.4**, this induces a canonical isomorphism:

$$H^n(G_w, L_w^*) \cong H^n(G_{w'}, L_{w'}^*).$$

Definition 15.2. For any $v \in V_K$, we define $G_v := G_w$ and $L_v := L_w$ for any choice of $w|v$.

Proposition 15.1. For all $n > 0$,

$$H^n(L/K, \mathbb{I}_L) = \bigoplus_{v \in V_K} H^n(G_v, L_v^*).$$

Proof. For all $v \in V_K$, we have the isomorphisms:

$$\prod_{w|v} L_w^* \cong \mathrm{Ind}_{G_v}^G(L_v^*) \quad \text{and} \quad \prod_{w|v} \mathcal{O}_{L_w}^* \cong \mathrm{Ind}_{G_v}^G \mathcal{O}_{L_v}^*.$$

By **Shapiro's Lemma**:

$$H^n\left(G, \prod_{w|v} L_w^*\right) \cong H^n(G_v, L_v^*)$$
$$H^n\left(G, \prod_{w|v} \mathcal{O}_{L_w}^*\right) \cong H^n(G_v, \mathcal{O}_{L_v}^*) = 0$$

where the second equality holds if L_v/K_v is unramified (from **Lemma 13.2**).

Let $V_{K,\infty} \subseteq S \subseteq V_K$ be a finite set containing all places that ramify in L. Define

$$\mathbb{I}_{L,S} = \prod_{v \in S} \left(\prod_{w|v} L_w^* \right) \times \prod_{v \notin S} \left(\prod_{w|v} \mathcal{O}_{L_w}^* \right).$$

Then $\mathbb{I}_L = \varinjlim_S \mathbb{I}_{L,S}$. Taking cohomology, we have:

$$\begin{aligned} H^n(G, \mathbb{I}_L) &= \varinjlim_S H^n(G, \mathbb{I}_{L,S}) = \varinjlim_S \prod_{v \in S} H^n(G_v, L_v^*) \\ &= \bigoplus_{v \in V_K} H^n(G_v, L_v^*). \end{aligned}$$

□

Remark: The proposition does not hold when $n = 0$ because $H^0(G_v, \mathcal{O}_{L_v}^*) = \mathcal{O}_{K_v}^* \neq 0$. However, $\hat{H}^0(G_v, \mathcal{O}_{L_v}^*) = 0$ when L_v/K_v is unramified. Indeed, the proposition holds for

Tate cohomology $\hat{H}^n$ for all $n \in \mathbb{Z}$. (I did not write the Tate cohomology version because we haven't stated the exchange of $\hat{H}$ and $\varinjlim$, but in fact it is correct).

Corollary 15.1.

1. $H^1(L/K, \mathbb{I}_L) = 0$ (immediately from **Hilbert 90**).
2. $H^2(L/K, \mathbb{I}_L) \cong \bigoplus_{v \in V_K} \mathrm{Br}(L_v/K_v)$.

Reason for introducing Tate-Nakayama Hypothesis: The ultimate goal of Global Class Field Theory is to establish the isomorphism (Artin Reciprocity):

$$C_K/N_{L/K}(C_L) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

In the language of Tate cohomology, noting that $\mathrm{Gal}(L/K)^{\mathrm{ab}} \cong \hat{H}^{-2}(G, \mathbb{Z})$, this is equivalent to establishing an isomorphism:

$$\hat{H}^0(G, C_L) \cong \hat{H}^{-2}(G, \mathbb{Z}).$$

The **Tate-Nakayama Theorem** is the algebraic machinery that guarantees the existence of such isomorphisms (specifically the cup product with a fundamental class) between the cohomology of a module A (here $A = C_L$) and the cohomology of $\mathbb{Z}$. However, this theorem applies *if and only if* the module satisfies specific conditions: vanishing of H^1 and the cyclic structure of H^2.

Therefore, verifying these hypotheses for the Idele Class Group C_L is the crucial step to proving the main theorems of Class Field Theory.

Hypothesis of Tate-Nakayama: Let $A = C_L = \mathbb{I}_L/L^*$. We hope:

1. $H^1(L/K, C_L) = 0$.
2. $H^2(L/K, C_L)$ is a cyclic group generated by one certain element of order $|\mathrm{Gal}(L/K)|$.

The verification of these hypotheses is not easy and the first one will be done in the next subsection.

15.2 Vanishing of $H^1(L/K, C_L)$ and second inequality

Proposition 15.2 (**Second Inequality**)**.** Let L/K be a finite Galois extension. Then

$$[C_K : N_{L/K}(C_L)] \leq [L : K].$$

We need to use a special case of the **generalized Dirichlet's Theorem** (i.e., equal distribution of ideals in $\mathrm{Cl}_{\mathfrak{m}}(K)$), whose proof uses analytic properties of Weber L-function $L_{K,\mathfrak{m}}(s,\chi)$. It is holomorphic at $s=1$ if $\chi \neq \mathrm{triv}$ and has a simple pole at $s=1$ if $\chi = \mathrm{triv}$.

Remark/Recall: We used Class Field Theory merely to prove $L(1,\chi) \neq 0$ for all $\chi \neq \mathrm{triv}$ via the factorization:

$$\zeta_{K_{\mathfrak{m}}}(s) = \zeta_K(s) \prod_{1 \neq \chi \in \widehat{\mathrm{Cl}}_{\mathfrak{m}}(K)} L_{K,\mathfrak{m}}(s,\chi).$$

where the existence of the Ray Class Field $K_{\mathfrak{m}}$ is also dependent on Class Field Theory.

Proposition 15.3. Let $\mathfrak{m}$ be a modulus of K. Let $H \leq \mathrm{Cl}_{\mathfrak{m}}(K)$ be the subgroup generated by $[\mathfrak{p}_v]^{f(w|v)}$ for all $v \nmid \mathfrak{m}_0$. Let

$$T := \{v \in V_{K,f} \mid \mathfrak{p}_v \nmid \mathfrak{m}_0, \overline{\mathfrak{p}}_v \in H \leq \mathrm{Cl}_{\mathfrak{m}}(K)\}.$$

Then the Dirichlet density of T is $\rho(T) = \frac{|H|}{|\mathrm{Cl}_{\mathfrak{m}}(K)|}$ and we have the inequality:

$$|\mathrm{Cl}_{\mathfrak{m}}(K)/H| \leq [L : K].$$

Proof of Proposition 15.3. We analyze the behavior of the Weber L-function as $s \to 1^+$.

$$\log L_{K,\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}_0} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}, \quad \forall \chi \in \widehat{\mathrm{Cl}_{\mathfrak{m}}(K)}.$$

Summing over all characters χ that are trivial on H (i.e., $\chi \in \widehat{\mathrm{Cl}_{\mathfrak{m}}(K)/H}$):

$$\begin{aligned}\sum_{\chi \in \widehat{\mathrm{Cl}_{\mathfrak{m}}(K)/H}} \log L_{K,\mathfrak{m}}(s,\chi) &\sim \sum_{\mathfrak{p} \nmid \mathfrak{m}_0} \frac{\sum_{\chi \in \widehat{\mathrm{Cl}_{\mathfrak{m}}(K)/H}} \chi(\mathfrak{p})}{N(\mathfrak{p})^s} \\ &\sim |\mathrm{Cl}_{\mathfrak{m}}(K)/H| \cdot \sum_{\substack{\mathfrak{p} \nmid \mathfrak{m}_0 \\ \overline{\mathfrak{p}} \in H}} \frac{1}{N(\mathfrak{p})^s} \quad \text{(by orthogonality of characters).}\end{aligned}$$

On the other hand, let $n_\chi = \mathrm{ord}_{s=1} L_{K,\mathfrak{m}}(s,\chi)$. The term for the trivial character contributes

$\log \frac{1}{s-1}$ (simple pole), while non-trivial characters contribute $-n_\chi \log \frac{1}{s-1}$. Thus:

$$\text{LHS} \sim \left(1 - \sum_{1 \neq \chi \in \widehat{\mathrm{Cl}_{\mathfrak{m}}(K)/H}} n_\chi\right) \log \frac{1}{s-1}.$$

Comparing the two expressions, we get the density:

$$\rho(T) = \frac{1 - \sum_{\chi \neq 1} n_\chi}{|\mathrm{Cl}_{\mathfrak{m}}(K)/H|}.$$

We know that the set of primes splitting completely in L, denoted $\mathrm{Spl}_{L/K}$, satisfies $\mathrm{Spl}_{L/K} \subseteq T \cup \{\text{finite set}\}$. This implies:

$$\rho(T) \geq \rho(\mathrm{Spl}_{L/K}) = \frac{1}{[L:K]} > 0.$$

(Note: Here we have not used Class Field Theory yet, see **Homework 8.4**).

Since the density must be positive, the numerator $1 - \sum n_\chi$ must be positive. Since $n_\chi \geq 0$ (as L-functions are holomorphic), we must have $n_\chi = 0$ for all $\chi \neq 1$. Therefore,

$$\rho(T) = \frac{1}{|\mathrm{Cl}_{\mathfrak{m}}(K)/H|}.$$

Finally, from the inequality of densities:

$$\frac{1}{|\mathrm{Cl}_{\mathfrak{m}}(K)/H|} \geq \frac{1}{[L:K]} \quad \Longrightarrow \quad |\mathrm{Cl}_{\mathfrak{m}}(K)/H| \leq [L:K]. \qquad \square$$

Proof of Proposition 15.2 (Second Inequality). By Local Class Field Theory (LCFT), $N_{L_w/K_v}(L_w^*) \subseteq K_v^*$ is an open subgroup. Moreover, if L_w/K_v is unramified, we have $N_{L_w/K_v}(\mathcal{O}_{L_w}^*) = \mathcal{O}_{K_v}^*$. This implies that $N_{L/K}(C_L) \subseteq C_K$ is an open subgroup. Therefore from **Homework 7.1**, there exists a modulus $\mathfrak{m}$ such that $N_{L/K}(C_L) \supseteq \overline{U}_{\mathfrak{m}}$.

Let $H := N_{L/K}(C_L)/\overline{U}_{\mathfrak{m}} \subseteq C_K/\overline{U}_{\mathfrak{m}} \cong \mathrm{Cl}_{\mathfrak{m}}(K)$. The isomorphism follows from **Proposition 7.2**, and the image of $N_{L/K}(C_L)/\overline{U}_{\mathfrak{m}}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is actually the subgroup generated by $[\mathfrak{p}_v]^{f(w/v)}$ for all $v \nmid \mathfrak{m}_0$.

Then, by **Proposition 15.3**:

$$[C_K : N_{L/K}(C_L)] = [\mathrm{Cl}_{\mathfrak{m}}(K) : H] \leq [L:K]. \qquad \square$$

Proposition 15.4. For L/K a cyclic Galois extension, the Herbrand quotient is $h(C_L) = [L : K]$.

Proof. Let $V_{L,\infty} \subseteq \tilde{S} \subseteq V_L$ be a finite set. Define

$$\mathbb{I}_{L,\tilde{S}} := \prod_{w \in \tilde{S}} L_w^* \times \prod_{w \notin \tilde{S}} \mathcal{O}_{L_w}^*.$$

Then $\mathbb{I}_L = \varinjlim_{\tilde{S}} \mathbb{I}_{L,\tilde{S}}$.

Claim: There exists a set $\tilde{S} \subseteq V_L$ such that:

1. $\tilde{S}$ is stable under the action of $G = \mathrm{Gal}(L/K)$.
2. $\tilde{S}$ contains $V_{L,\infty}$ and all primes that ramify in L/K.
3. $\mathbb{I}_L = \mathbb{I}_{L,\tilde{S}} \cdot L^*$.

We have the exact sequence:

$$0 \longrightarrow C_L^1 \longrightarrow C_L \xrightarrow{||\cdot||} \mathbb{R}_{>0} \longrightarrow 0,$$

where C_L^1 is compact. Let $\theta : \mathbb{I}_L \to C_L$ be the quotient map. We have $C_L = \bigcup_{\tilde{S}} \theta(\mathbb{I}_{L,\tilde{S}})$, and each $\theta(\mathbb{I}_{L,\tilde{S}})$ is open. Since C_L^1 is compact, there exists a set $\tilde{S}$ such that $C_L^1 \subseteq \theta(\mathbb{I}_{L,\tilde{S}})$. The map $\theta(\mathbb{I}_{L,\tilde{S}}) \xrightarrow{||\cdot||} \mathbb{R}_{>0}$ is surjective. Therefore, $\theta(\mathbb{I}_{L,\tilde{S}}) = C_L$, which implies $\mathbb{I}_L = \mathbb{I}_{L,\tilde{S}} \cdot L^*$. The claim follows.

Thus, we have the isomorphism:

$$C_L \cong \mathbb{I}_L / L^* \cong \mathbb{I}_{L,\tilde{S}} / (\mathbb{I}_{L,\tilde{S}} \cap L^*).$$

Note that $\mathbb{I}_{L,\tilde{S}} \cap L^* = \mathcal{O}_{L,\tilde{S}}^*$. By **Homework 12.4(c)**, we know that

$$h(\mathcal{O}_{L,\tilde{S}}^*) = \frac{\prod_{v \in S} n_v}{[L : K]},$$

where $S = \pi(\tilde{S})$ with $\pi : V_L \to V_K$, and $n_v = [L_v : K_v]$. Thus, it suffices to show that $h(\mathbb{I}_{L,\tilde{S}}) = \prod_{v \in S} n_v$. By **Proposition 15.1**, we have the decomposition of cohomology:

$$H^n(L/K, \mathbb{I}_{L,\tilde{S}}) = \bigoplus_{v \in S} H^n(L_v/K_v, L_v^*).$$

It suffices to show that $h(L_v^*) = n_v$ as a $\mathrm{Gal}(L_v/K_v)$-module. Notice that $\mathrm{Gal}(L_v/K_v)$ is also cyclic by the assumption on L/K. This follows from **Proof of Step 3 of Theorem**

13.2. □

Corollary 15.2. For L/K a cyclic Galois extension, we have:

$$[C_K : N_{L/K}(C_L)] = [L : K] \quad \text{and} \quad H^1(L/K, C_L) = 0.$$

Proof. We have the following calculation for the Herbrand quotient:

$$h(C_L) = \frac{|\hat{H}^0(L/K, C_L)|}{|\hat{H}^1(L/K, C_L)|} \leq |\hat{H}^0(L/K, C_L)| = [C_K : N_{L/K}(C_L)].$$

By the **second inequality** $h(C_L) \leq [C_K : N_{L/K}(C_L)] \leq [L : K]$. Since $h(C_L) = [L : K]$, we must have $|\hat{H}^1(L/K, C_L)| = 1$ and equality in the index. □

Theorem 15.1. Let L/K be a finite Galois extension. Then $H^1(L/K, C_L) = 0$.

Proof. (We have already proved this for cyclic extensions).

Step 1. It suffices to prove the theorem in the case where $G = \mathrm{Gal}(L/K)$ is a p-group. Let $G_p \leq G = \mathrm{Gal}(L/K)$ be a Sylow p-subgroup. **Recall:** The restriction map $\mathrm{Res} : H^1(G, C_L) \longrightarrow H^1(G_p, C_L)$ is injective on the p-primary components. If $H^1(G_p, C_L) = 0$ for all p, then $H^1(G, C_L) = 0$.

Step 2. We prove the case where G is a p-group. We prove by induction on $|G|$. If $|G| = p$, then G is cyclic, which is OK. In general, there exists a normal subgroup $H \trianglelefteq G$ which is nontrivial, as G has a nontrivial center. Consider the inflation-restriction exact sequence:

$$0 \longrightarrow H^1(G/H, C_L^H) \xrightarrow{\mathrm{Inf}} H^1(G, C_L) \xrightarrow{\mathrm{Res}} H^1(H, C_L)$$

Note that $C_L^H = C_E$ where $E = L^H$, so $G/H = \mathrm{Gal}(E/K)$. By the induction hypothesis, $H^1(G/H, C_E) = 0$. Also, $H^1(H, C_L) = 0$ (since H is a smaller p-group). Therefore,

$$H^1(G, C_L) = 0.$$ □

15.3 Artin Reciprocity

Let L/K be a finite Galois extension. From **Proposition 15.1**, we have the isomorphism:

$$H^2(G, \mathbb{I}_L) \cong \bigoplus_{v \in V_K} \mathrm{Br}(L_w/K_v) \xrightarrow{\mathrm{inv}} \bigoplus_{v \in V_K} \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

Definition 15.3.

1. We define the **invariant map** $\mathrm{inv}_{L/K} : H^2(G, \mathbb{I}_L) \longrightarrow \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ by:

$$x = (x_v)_{v \in V_K} \longmapsto \sum_{v \in V_K} \mathrm{inv}_{K_v}(x_v).$$

2. We define the **global Artin map** $\psi_{L/K} : \mathbb{I}_K \longrightarrow G^{\mathrm{ab}}$ as follows: For each $v \in V_K$, fix a place $w|v$. We have the natural homomorphism induced by the inclusion:

$$j_v : \mathrm{Gal}(L_v/K_v)^{\mathrm{ab}} \longrightarrow G^{\mathrm{ab}}.$$

(Note: This map is not necessarily injective). Then define:

$$x = (x_v)_v \longmapsto \prod_{v \in V_K} j_v(\psi_{L_v/K_v}(x_v)).$$

(Note: The image in G^{ab} is independent of the choice of $w|v$ because conjugate elements are equal in the abelianization).

Remark:

1. $\psi_{L/K}$ is well-defined.

   By Local Class Field Theory (LCFT), if L_v/K_v is unramified, then

$$\mathcal{O}_{K_v}^* = N_{L_v/K_v}(\mathcal{O}_{L_v}^*) \subseteq N_{L_v/K_v}({L_v}^*) = \ker \psi_{L_v/K_v}$$

   So $\psi_{L_v/K_v}(\mathcal{O}_{L_v}^*) = 1$.

   Recall that $\mathbb{I}_K = \varinjlim_S \mathbb{I}_{K,S}$, where S runs through finite sets containing $V_{K,\infty}$ and all primes ramified in L/K. For any $x = (x_v) \in \mathbb{I}_{K,S}$, we have $x_v \in \mathcal{O}_{K_v}^*$ for $v \notin S$. Since primes outside S are unramified, the local Artin map is trivial on these components. Then $\psi_{L/K}(x) = \prod_{v \in S} j_v(\psi_{L_v/K_v}(x_v))$, which is a finite product.

2. $\psi_{L/K}$ is continuous. The subgroup

$$\prod_{v \in S} \ker \psi_{L_v/K_v} \times \prod_{v \notin S} \mathcal{O}_{K_v}^* \subseteq \ker \psi_{L/K}$$

   is open in $\mathbb{I}_K$.

Proposition 15.5. For all $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ and for all $a \in \mathbb{I}_K$, we have:

$$\chi(\psi_{L/K}(a)) = \mathrm{inv}_{L/K}(a \cup \delta\chi)$$

where $a \in \hat{H}^0(G, \mathbb{I}_L)$ and $\delta\chi \in H^2(G, \mathbb{Z})$.

Proof. Apply the local formula. □

Proposition 15.6.

1. Let $M \supseteq L \supseteq K$ with M/K a finite Galois extension. Then the following diagram commutes:

$$\begin{array}{ccc} H^2(M/L, \mathbb{I}_M) & \xrightarrow{\mathrm{inv}_{M/L}} & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z} \\ \Big\uparrow{\scriptstyle \mathrm{Res}} & & \Big\uparrow{\scriptstyle \cdot[L:K]} \\ H^2(M/K, \mathbb{I}_M) & \xrightarrow{\mathrm{inv}_{M/K}} & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \end{array} \qquad \begin{array}{ccc} H^2(M/L, \mathbb{I}_M) & \xrightarrow{\mathrm{inv}_{M/L}} & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow \\ H^2(M/K, \mathbb{I}_M) & \xrightarrow{\mathrm{inv}_{M/K}} & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

2. If L/K is Galois, then we have the commutative diagram:

$$\begin{array}{ccc} H^2(L/K, \mathbb{I}_L) & \xrightarrow{\mathrm{Inf}} & H^2(M/K, \mathbb{I}_M) \\ & \searrow^{\mathrm{inv}_{L/K}} & \Big\downarrow{\scriptstyle \mathrm{inv}_{M/K}} \\ & & \mathbb{Q}/\mathbb{Z} \end{array}$$

Remark: You may confuse why does the global degree $[L : K]$ appear in the diagram, whereas local theory involves $[L_w : K_v]$? That is because the global cohomology is a direct sum $\bigoplus_{v \in V_K}$. The global factor $[L : K]$ arises from summing the local contributions, using the fundamental identity $\sum_{w|v}[L_w : K_v] = [L : K]$.

Let L/K be a finite abelian extension.

Theorem 15.2. $\psi_{L/K}(a) = 1$ for all $a \in K^* \subseteq \mathbb{I}_K$. Equivalently, $\psi_{L/K}$ factors through $C_K \longrightarrow G$.

Theorem 15.3. The invariant map $\mathrm{inv} : H^2(L/K, \mathbb{I}_L) \longrightarrow \mathbb{Q}/\mathbb{Z}$ is zero on the image of

$$H^2(L/K, L^*) \longrightarrow H^2(L/K, \mathbb{I}_L).$$

Remark: As $H^1(L/K, C_L) = 0$, the map $H^2(L/K, L^*) \longrightarrow H^2(L/K, \mathbb{I}_L)$ is injective. We have the identifications:

$$H^2(L/K, L^*) = \mathrm{Br}(L/K) \quad \text{and} \quad H^2(L/K, \mathbb{I}_L) = \bigoplus_{v \in V_K} \mathrm{Br}(L_v/K_v).$$

We will prove the two theorems together later.

Corollary 15.3. Let L/K be a finite abelian extension. Then $\psi_{L/K}$ is surjective with $\ker \psi_{L/K} = N_{L/K}(C_L)$.

Proof of Corollary 15.3. (1) First, we show that $\psi_{L/K}$ is surjective. Let $H \subseteq G = \mathrm{Gal}(L/K)$ be the subgroup generated by $\mathrm{Frob}_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}_v}\right)$ for all $v \in V_{K,f}$ that are unramified in L. By **Proposition 14.2**, $H \subseteq \mathrm{Im}(\psi_{L/K})$.

We will show that $H = G$. Let $E = L^H$. Then

$$\left(\frac{E/K}{\mathfrak{p}_v}\right) = \left(\frac{L/K}{\mathfrak{p}_v}\right)\Bigg|_E = 1 \in \mathrm{Gal}(E/K).$$

This implies that the density of split primes is $\rho(\mathrm{Spl}_{E/K}) = 1$. Since $\rho(\mathrm{Spl}_{E/K}) = \frac{1}{[E:K]}$, we have $E = K$, and therefore $H = G$.

(2) By LCFT, we have $N_{L/K}(C_L) \subseteq \ker \psi_{L/K}$. This induces a surjective map:

$$C_K/N_{L/K}(C_L) \longrightarrow G.$$

By the **Second Inequality**, $[C_K : N_{L/K}(C_L)] \leq [L : K] = |G|$. Since we have a surjective map from a group of order at most $|G|$ to a group of order $|G|$, it must be an isomorphism. □

Strategy to prove Theorem 15.2 and Theorem 15.3.

- **Step 1:** Theorem 15.2 holds for cyclotomic extensions. (L/K is called cyclotomic if $L \subseteq K(\zeta_n)$ for some n).
- **Step 2:**
  1. If Theorem 15.3 holds for L/K, then Theorem 15.2 holds for L/K.
  2. If L/K is cyclic, then if Theorem 15.2 holds for L/K, Theorem 15.3 holds for L/K.

- **Step 3:** If Theorem 15.3 holds for cyclic cyclotomic extensions, then it is true for all finite abelian extensions L/K.

□

Proof of Step 1. $L \subseteq K(\zeta_n)$ for some n. We may assume $L = K(\zeta_n)$. This is justified by the following commutative diagram:

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\psi_{K(\zeta_n)/K}} & \mathrm{Gal}(K(\zeta_n)/K) \\ & \searrow^{\psi_{L/K}} & \downarrow \\ & & \mathrm{Gal}(L/K) \end{array}$$

We may assume $K = \mathbb{Q}$. By Local Class Field Theory (LCFT), we have the local diagram, which implies the global diagram:

$$\begin{array}{ccc} K_v^* & \xrightarrow{\psi} & \mathrm{Gal}(K_v(\zeta_n)/K_v) \\ {\scriptstyle N_{K_v/\mathbb{Q}_p}}\downarrow & & \downarrow \\ \mathbb{Q}_p^* & \xrightarrow{\psi} & \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \end{array} \quad \Longrightarrow \quad \begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\psi} & \mathrm{Gal}(K(\zeta_n)/K) \\ {\scriptstyle N}\downarrow & & \downarrow \\ \mathbb{I}_{\mathbb{Q}} & \xrightarrow{\psi} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \end{array}$$

We may assume $n = p^r$. This follows from the decomposition:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_i \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i}^{r_i})/\mathbb{Q}).$$

It suffices to show that the map $\psi : \mathbb{I}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ satisfies:

$$\psi(a) = 1 \quad \forall a \in \mathbb{Q}^*$$

by explicit computation! □

Proof of Step 2(1). We want to show that $\psi_{L/K}(a) = 1$ for all $a \in K^*$. It suffices to show that for all $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$, we have $\chi(\psi_{L/K}(a)) = 0$. We have:

$$\mathrm{LHS} = \mathrm{inv}_{L/K}(\underbrace{a}_{\in \hat{H}^0(L/K, L^*)} \cup \underbrace{\delta\chi}_{\in H^2(L/K, \mathbb{Z})}) = 0.$$

This holds because the element $a \cup \delta\chi$ belongs to $\mathrm{Br}(L/K)$, and by Theorem 15.3, the invariant map is zero on the image of $\mathrm{Br}(L/K)$. □

Proof of Step 2(2). Assume L/K is cyclic. Choose an injective character $\chi : G \longrightarrow \mathbb{Q}/\mathbb{Z}$. Then we have an isomorphism from **Homework 12.1**:

$$\hat{H}^i(G, L^*) \xrightarrow[\cong]{-\cup\delta\chi} \hat{H}^{i+2}(G, L^*).$$

By cyclic case of Theorem 15.2, we have:

$$\chi(\psi_{L/K}(a)) = 0 \quad \forall a \in K^*.$$

This can be written as:

$$\mathrm{inv}_{L/K}(\underbrace{a \cup \delta\chi}_{\in \mathrm{Br}(L/K)}) = 0.$$

Since the map $- \cup \delta\chi$ is an isomorphism, the term $a \cup \delta\chi$ can take all values in $\mathrm{Br}(L/K)$ as a varies. Therefore, the invariant map is zero on $\mathrm{Br}(L/K)$, which proves cyclic case of Theorem 15.3. □

Before proving Step 3, we state one lemma and one proposition.

Lemma 15.1. Let $S \subseteq V_{K,f}$ be a finite set and let $m > 0$. Then there exists a totally complex, cyclic cyclotomic extension $\tilde{L}/K$ such that $m \mid [\tilde{L}_v : K_v]$ for all $v \in S$.

Proof of Lemma. **Step 1:** We may assume $K = \mathbb{Q}$.

Suppose we have proved the lemma for $(\mathbb{Q}, \bar{S}, m[K : \mathbb{Q}])$, where $\bar{S} = \pi(S)$ and $\pi : V_K \longrightarrow V_{\mathbb{Q}}$ is the natural restriction map. That is, there exists a totally complex cyclic cyclotomic extension $L/\mathbb{Q}$ such that

$$m[K : \mathbb{Q}] \mid [L_p : \mathbb{Q}_p] \quad \forall p \in \bar{S}.$$

Let $\tilde{L} = L \cdot K$. Then $\tilde{L}/K$ is totally complex cyclotomic extension $L \subseteq \widetilde{L} = L \cdot K$. We have the diagram of fields:

$$\begin{array}{ccc} L & \subseteq & \widetilde{L} \\ \cup & & \cup \\ \mathbb{Q} & \subseteq & K \end{array} \quad \text{and locally} \quad \begin{array}{ccc} L_p & \subseteq & \widetilde{L}_v \\ \cup & & \cup \\ \mathbb{Q}_p & \subseteq & K_v \end{array} \quad \text{for } v|p.$$

This implies:

$$\begin{aligned} & [L_p : \mathbb{Q}_p] \mid [\widetilde{L}_v : \mathbb{Q}_p] \\ \Longrightarrow\ & m \cdot [K : \mathbb{Q}] \mid [\widetilde{L}_v : K_v][K_v : \mathbb{Q}_p] \\ \Longrightarrow\ & m \mid [\widetilde{L}_v : K_v]. \end{aligned}$$

Step 2: Case $K = \mathbb{Q}$. This follows from explicit computation in cyclotomic extensions. (Reference: Cassels-Fröhlich, VII. §10, Lemma on page 192). □

By the Lemma, we can prove the following proposition.

Proposition 15.7.

$$\mathrm{Br}(K) = \bigcup_{\substack{L/K \text{ cyclic} \\ \text{cyclotomic}}} \mathrm{Br}(L/K)$$

Proof of Proposition. **Recall:** We have the exact sequence:

$$0 \longrightarrow \mathrm{Br}(L/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

For any $\alpha \in \mathrm{Br}(K)$, we want to find a cyclic cyclotomic extension L/K such that $\mathrm{Res}(\alpha) = 0$.

In fact: We have the following commutative diagram:

$$\begin{array}{ccccc} 0 \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_{v \in V_K} \mathrm{Br}(K_v) & \qquad \alpha \longmapsto (\alpha_v)_v \\ & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & \\ & \mathrm{Br}(L) & \longrightarrow & \bigoplus_{w \in V_L} \mathrm{Br}(L_w) & \end{array}$$

It suffices to show that $\mathrm{Res}(\alpha_v) = 0$ for all $v \in V_K$, which:

$$\begin{aligned} & \Longleftrightarrow \mathrm{inv}(\mathrm{Res}(\alpha_v)) = 0 \quad \forall v \in V_K \\ & \Longleftrightarrow [L_w : K_v] \cdot \mathrm{inv}(\alpha_v) = 0 \text{ in } \mathbb{Q}/\mathbb{Z}. \end{aligned}$$

The first " $\Longleftrightarrow$ " comes from $\mathrm{inv} : \mathrm{Br}(L_w) \to \mathbb{Q}/\mathbb{Z}$ being an isomorphism. The second " $\Longleftrightarrow$ " comes from the compatibility of the invariant map with respect to the restriction map, which multiplies the invariant by the local degree $[L_w : K_v]$.

Let $S := \{v \in V_{K,f} \mid \alpha_v \neq 0\}$. This is a finite set. There exists $m \in \mathbb{Z}_{>0}$ such that $m \cdot \mathrm{inv}(\alpha_v) = 0$ for all $v \in S$. It suffices to find a totally complex cyclic cyclotomic extension L/K such that $m \mid [L_w : K_v]$ for all $v \in S$, which is **Lemma 15.1**. □

Remark: The condition that L is *totally complex* ensures that for every real place v of K, the local extension is $L_w/K_v \cong \mathbb{C}/\mathbb{R}$. This provides the necessary factor of $[L_w : K_v] = 2$ to annihilate any non-trivial local invariant at infinity (which is always $1/2$).

Proof of Step 3. Immediately from **Proposition 15.7**. □

.

A Some completion of details

If you wanna use citations of the context, use in the following form:

- hypertarget{label-1}{xxxx}
- xxxx
- hyperlink{label-1}{xxxx}

Proof of Proposition 9.1

Should discuss left/right modules carefully.
For the first isomorphism:

$$\begin{aligned}\mathrm{Hom}_G(A, \mathrm{Ind}_H^G A') &= \mathrm{Hom}_{\mathbb{Z}[G]}({}_{\mathbb{Z}[G]}A, {}_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}[H]}({}_{\mathbb{Z}[H]}\mathbb{Z}[G]_{\mathbb{Z}[G]}, {}_{\mathbb{Z}[H]}A')) \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}({}_{\mathbb{Z}[G]}A \otimes_{\mathbb{Z}[G]} {}_{\mathbb{Z}[H]}\mathbb{Z}[G]_{\mathbb{Z}[G]}, {}_{\mathbb{Z}[H]}A') \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}({}_{\mathbb{Z}[H]}A, {}_{\mathbb{Z}[H]}A') \\ &= \mathrm{Hom}_H(\mathrm{Res}_H^G A, A')\end{aligned}$$

For the second isomorphism:

$$\begin{aligned}\mathrm{Hom}_G(\mathrm{ind}_H^G A', A) &= \mathrm{Hom}_{\mathbb{Z}[G]}({}_{\mathbb{Z}[G]}\mathbb{Z}[G]_{\mathbb{Z}[H]} \otimes_{\mathbb{Z}[H]} {}_{\mathbb{Z}[H]}A', {}_{\mathbb{Z}[G]}A) \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}({}_{\mathbb{Z}[H]}A', {}_{\mathbb{Z}[H]}\mathrm{Hom}_{\mathbb{Z}[G]}({}_{\mathbb{Z}[G]}\mathbb{Z}[G]_{\mathbb{Z}[H]}, {}_{\mathbb{Z}[G]}A)) \\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}({}_{\mathbb{Z}[H]}A', {}_{\mathbb{Z}[H]}A) \\ &= \mathrm{Hom}_H(A', \mathrm{Res}_H^G A)\end{aligned}$$

Detail in Proposition 10.1

We need to explain why $\varinjlim_j \mathrm{Ind}_{\{e\}}^G A_j \cong \mathrm{Ind}_{\{e\}}^G(\varinjlim_j A_j)$.
By definition of the coinduction functor, this is equivalent to proving:

$$\varinjlim_j \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A_j) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \varinjlim_j A_j)$$

This commutation holds if and only if the module $\mathbb{Z}[G]$ is a finitely presented $\mathbb{Z}$-module.

We verify this condition. The problem states that G is a **finite group**. Let $|G| = n$. As a $\mathbb{Z}$-module (an abelian group), the group ring $\mathbb{Z}[G]$ is the free abelian group with the elements of G as a basis. Since the basis is finite, $\mathbb{Z}[G]$ is a finitely generated free $\mathbb{Z}$-module of rank n.

Every finitely generated free module is finitely presented. Therefore, the condition holds, and the Hom-functor commutes with the direct limit functor. This establishes the required isomorphism. The finiteness of G is the crucial hypothesis.

For $i = 0$, we need to prove the Hom functor commutes with the direct limit:

$$\mathrm{Hom}_G(\mathbb{Z}, \varinjlim_j A_j) \cong \varinjlim_j \mathrm{Hom}_G(\mathbb{Z}, A_j)$$

This commutation holds if the module $\mathbb{Z}$ is a finitely presented $\mathbb{Z}[G]$-module. We verify this condition.

Consider the augmentation map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$, a surjective G-module homomorphism. Its kernel is the augmentation ideal, I_G. This gives a short exact sequence of G-modules:

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

This is the beginning of a free resolution for $\mathbb{Z}$. To show $\mathbb{Z}$ is finitely presented, we must show that I_G is a finitely generated $\mathbb{Z}[G]$-module.

The augmentation ideal I_G is generated as a $\mathbb{Z}[G]$-module by the set $\{g - 1 \mid g \in G\}$. Since the group G is **finite**, this is a finite set of generators. Therefore, I_G is a finitely generated $\mathbb{Z}[G]$-module.

Since $\mathbb{Z}[G]$ is a free (and thus finitely generated) $\mathbb{Z}[G]$-module of rank 1, and its kernel I_G is finitely generated, we have constructed a finite presentation for $\mathbb{Z}$.

Because $\mathbb{Z}$ is a finitely presented $\mathbb{Z}[G]$-module, the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ commutes with direct limits. This proves the required isomorphism for $i = 0$.

Completion of the proof of Lemma 15.1

Proof of Step 2 (Explicit Construction):

It suffices to construct such a field L in the case $K = \mathbb{Q}$ (by replacing m with $m[K : \mathbb{Q}]$ as shown in Step 1). Let $m = q_1^{e_1} \cdots q_k^{e_k}$ be the prime factorization of m. We will construct cyclic extensions for each prime power.

Case 1: q is an odd prime. Take r sufficiently large. Consider the cyclotomic extension $L(q) = \mathbb{Q}(\zeta_{q^r})$. Its Galois group is:

$$\mathrm{Gal}(L(q)/\mathbb{Q}) \cong (\mathbb{Z}/q^r\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/q^{r-1}\mathbb{Z}.$$

Let $L'(q)$ be the subfield corresponding to the cyclic factor of order q^{r-1}. Then $L'(q)/\mathbb{Q}$ is a cyclic cyclotomic extension of degree q^{r-1}, and $[L(q) : L'(q)] = q - 1$. For any fixed prime

$p \in S$ (where $p \neq \infty$), we localize at p. Since any finite extension of $\mathbb{Q}_p$ contains only a finite number of roots of unity, the local degree $[L(q)_p : \mathbb{Q}_p] \to \infty$ as $r \to \infty$. Since $[L'(q)_p : \mathbb{Q}_p]$ is always a power of q and $[L(q)_p : L'(q)_p]$ divides $q-1$ (which is coprime to q), the local degree $[L'(q)_p : \mathbb{Q}_p]$ must grow to infinity as $r \to \infty$. Thus, for large enough r, $[L'(q)_p : \mathbb{Q}_p]$ is divisible by any required power of q.

Case 2: $q = 2$**.** Take r large and let $L(2) = \mathbb{Q}(\zeta_{2^r})$.

$$\mathrm{Gal}(L(2)/\mathbb{Q}) \cong (\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}.$$

We need a *totally complex* cyclic subfield. Let ζ be a primitive 2^r-th root of unity and set $\xi = \zeta - \zeta^{-1}$. Let $L'(2) = \mathbb{Q}(\xi)$. The automorphisms of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are of the form $\sigma_\mu : \zeta \mapsto \zeta^\mu$ for μ odd. Then $\sigma_\mu(\xi) = \zeta^\mu - \zeta^{-\mu}$. Note that $\sigma_{-1}(\xi) = \zeta^{-1} - \zeta = -\xi$. Thus $\mathbb{Q}(\xi)$ is not real (so the local degree at ∞ is 2). One can check that $\mathrm{Gal}(L'(2)/\mathbb{Q})$ corresponds to the subgroup of $\mu \equiv 1 \pmod 4$, which is cyclic of order 2^{r-2}. Since $[L(2) : L'(2)] = 2$, the same argument as in the odd case shows that for any finite prime p, we can make $[L'(2)_p : \mathbb{Q}_p]$ divisible by an arbitrarily large power of 2 by taking r large enough.

Conclusion: Let L be the compositum of $L'(q_1), \ldots, L'(q_k)$ (and $L'(2)$ if $2|m$) for sufficiently large r. Since these fields correspond to different primes, they are linearly disjoint, and the Galois group of the compositum is the direct product of the individual Galois groups. Thus, $L/\mathbb{Q}$ is a cyclic cyclotomic extension. It is totally complex (due to the $L'(2)$ factor or because it contains complex subfields). Finally, for every $p \in S$, the local degree $[L_p : \mathbb{Q}_p]$ is divisible by the local degrees of its components, hence divisible by m. □

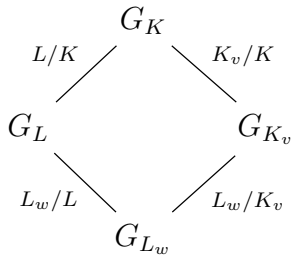
The origin of the commutative diagram in Proposition 15.7

Definition (Localization Map): For each place $v \in V_K$, the inclusion $K \hookrightarrow K_v$ induces a homomorphism on the Brauer groups $\mathrm{loc}_v : \mathrm{Br}(K) \to \mathrm{Br}(K_v)$. A fundamental fact of Hasse principles states that for any $\alpha \in \mathrm{Br}(K)$, $\mathrm{loc}_v(\alpha) = 0$ for almost all v. Thus, we have a well-defined map:

$$\mathrm{Br}(K) \longrightarrow \bigoplus_{v \in V_K} \mathrm{Br}(K_v), \quad \alpha \longmapsto (\mathrm{loc}_v(\alpha))_v.$$

Justification for Commutativity: The commutativity relies on the **transitivity of restriction** in group cohomology. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. We have the following inclusions

of subgroups corresponding to the fields:



For a cocycle $f \in Z^2(G_K, \bar{K}^*)$, the maps in the diagram correspond to restricting the domain of f:

- **Path 1 (Global then Local):** First restrict to G_L, then to G_{L_w}. The result is $f|_{G_{L_w}}$.
- **Path 2 (Local then Global):** First restrict to G_{K_v}, then to G_{L_w}. The result is also $f|_{G_{L_w}}$.

Since the resulting cocycles are identical, the diagram of cohomology groups commutes.

Justification for Injectivity: By the Remark, for all L/K finite Galois extension, we have the following exact sequence:

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_{v \in V_K} \mathrm{Br}(L_v/K_v)$$

Passing to direct limits we will have:

$$0 \to \mathrm{Br}(K) \to \bigoplus_{v \in V_K} \mathrm{Br}(K_v)$$