Class Field Theory - Milne

https://phanpu.github.io/

February 2023

Contents

1 Local Class Theory: Lubin-Tate Theory

Proposition 1.0.1. A local field K is a field that is locally compact with respect to a nontrivial absolute value. Thus it is

- a finite extension of $\mathbb{Q}_p$ for some p
- a finite extension of the field of Laurent series $\mathbb{F}_p((T))$
- $\mathbb{R}$ or $\mathbb{C}$

Remark 1.0.2. *Some notations: when K is non-Archimedean, its residue field has characteristic $p > 0$ and order q (a power of p), the ring of integers in K is denoted by $\mathcal{O}_K$ (or A), its maximal ideal by $\mathfrak{m}_K$ (or just $\mathfrak{m}$), and its group of units by $\mathcal{O}_K^*$ (or U_K). A generator (note that $\mathcal{O}_K$ is an DVR and hence is a PID) of $\mathfrak{m}$ is called a prime element of K (or a uniformizer or a local uniformizing parameter). If π is a prime element of K, then every $a \in K^*$ can be written uniquely as the form $a = u\pi^m$ with $u \in \mathcal{O}_K^*$ and $m \in \mathbb{Z}$. Hence $K^* = \mathcal{O}_K^* \times \pi^{\mathbb{Z}}$. We define $\mathrm{ord}_K(a) = m$. The normalized absolute value on K is defined by $|a| = q^{-\mathrm{ord}_K(a)}$.*

We let K^{al} denote a fixed algebraic closure of K (or separable algebraic closure in the case that K has characteristic $p > 0$). Both ord_K and $|\cdot|$ have unique extensions on K^{al}. Let K^{ab} denote the union of all Abelian finite extension of K, it is again a Abelian extension with Galois group is the quotient of $\mathrm{Gal}(K^{\mathrm{al}}/K)$ by the closure of its commutator subgroup.

1.1 Statements of the Main Theorems

Proposition 1.1.1. Let L be a finite unramified extension of K. Then $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$ and hence is cyclic, generated by the unique element $\sigma = \mathrm{Frob}_{L/K}$ such that $\sigma\alpha \equiv \alpha^q (\mathrm{mod}\ \mathfrak{m}_L)$ for all $\alpha \in \mathcal{O}_L$, where $q = |\mathcal{O}_K/\mathfrak{m}_K|$.

Theorem 1.1.2 (Local Reciprocity Law)**.** For every non-Archimedean local field K, there exists a unique homomorphism

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

with the following properties:

- for every prime element π of K and every finite unramified extension L of K, $\phi_K(\pi)$ acts on L as $\mathrm{Frob}_{L/K}$.
- for every finite Abelian extension L of K, $\mathrm{Nm}_{L/K}(L^*)$ is contained in the kernel of $\mathfrak{a} \mapsto \phi_K(a)|_L$, and ϕ_K induces an isomorphism

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

  In particular $(K^* : \mathrm{Nm}_{L/K}(L^*)) = [L : K]$.

We call ϕ_K and $\phi_{L/K}$ the local Artin maps for K and L/K. They are often also called the local reciprocity mas and denoted by rec_K and $\mathrm{rec}_{L/K}$, and $\phi_{L/K}$ is often called the norm residue map or symbol and denoted $a \mapsto (a, L/K)$.

Remark 1.1.3. *The right hands of the isomorphisms*

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

form an inverse system $(\mathrm{Gal}(L/K), \supseteq)$*. Therefore, there is an isomorphism between the completion of the left hand and the inverse limit*

$$\hat{\phi}_K : \widehat{K^*} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

where the topology of the completion $\widehat{K^*}$ *is determined by the fundamental system of neighborhoods of 1 formed by the norm groups. This topology is called by the norm topology.*

Remark 1.1.4. *If* $L = K^{\mathrm{un}}$ *the unramified closure of* K*, clearly we have*

$$\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \mathrm{Gal}(\bar{k}/k) \cong \varprojlim(\mathbb{Z}/n\mathbb{Z}) = \hat{\mathbb{Z}}$$

Then the first condition can be re-stated as: $\phi_K(\pi)$ *act as* Frob_K *on* K^{un}*, where* $\mathrm{Frob}_K \mapsto \sigma : (x \mapsto x^q)$*.*

Remark 1.1.5. *When* L/K *is finite and unramified,* $\mathrm{Gal}(L/K)$ *is a cyclic group generated by* $\phi_K(\pi)|_L = \mathrm{Frob}_{L/K}$*, thus for any* $a = u\pi^k \in K^*$ *(*$u \in \mathcal{O}_K^*, k \in \mathbb{Z}$*) we have* $\phi_K(a)|_L = \mathrm{Frob}_{L/K}^k$*. In particular, for* $a \in \mathcal{O}_K^*$*,* $\phi_K(a)|_L$ *acts trivially on* L*, that is,* $\mathcal{O}_K^* \subseteq \ker(\phi_{L/K}) = \mathrm{Nm}_{L/K}(L^*)$*.*

Note that

$$\mathcal{O}_K^* \supseteq 1 + \mathfrak{m}_K \supseteq 1 + \mathfrak{m}_K^2 \supseteq \cdots$$

form a fundamental system of neighborhoods of 1 in $\mathcal{O}_K^*$*. If a finite Abelian extension* L *is unramified over* K*, then we say* L/K *has conductor 0. Otherwise, the smallest* f *such that* $1 + \mathfrak{m}^f \subseteq \ker(\phi_{L/K})$ *is called the conductor of* L/K*.*

In the following we will introduce the local existence theorem, and then we obtain a fundamental system of neighborhoods of 1

$$\begin{aligned} &(1 + \mathfrak{m}^n) \cdot \langle \pi^m \rangle \cong (1 + \mathfrak{m}^n) \times m\mathbb{Z} \\ \subseteq\ & K^* = \mathcal{O}_K^* \cdot \pi^{\mathbb{Z}} \cong \mathcal{O}_K^* \times \mathbb{Z} \end{aligned}$$

then $\widehat{K^*} \cong \mathcal{O}_K^* \times \hat{\mathbb{Z}}$*. The identify map*

$$K^*(\textit{the usual topology}) \to K^*(\textit{the norm topology})$$

is continuous, thus there is a natural commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & K^* & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & \widehat{K^*} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

The decomposition $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \widehat{K^*} = \mathcal{O}_K^* \cdot \pi^{\hat{\mathbb{Z}}}$ *depends on the choice of* π*. If we fix a prime element* π*, then* K^{ab} *has the decomposition*

$$K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$$

where K_π is the subfield fixed by $\phi_K(\pi)$ and K^{un} is exactly the field fixed by $\phi_K(\mathcal{O}_K^*)$. Clearly K_π is the union of all finite Abelian extensions L/K such that $\pi \in \mathrm{Nm}(L^*)$. For example.

$$\mathbb{Q}_p^{\mathrm{ab}} = (\bigcup_n \mathbb{Q}[\zeta_{p^n}]) \cdot (\bigcup_{(m,p)=1} \mathbb{Q}[\zeta_m])$$

Corollary 1.1.6. (a) The map $L \mapsto \mathrm{Nm}(L^*)$ is a bijection from the set of finite Abelian extensions of K onto the set of norm groups in K^*.

(b) $L \subseteq L' \iff \mathrm{Nm}(L') \supseteq \mathrm{Nm}(L)$

(c) $\mathrm{Nm}((L \cdot L')^*) = \mathrm{Nm}(L) \cap \mathrm{Nm}(L')$

(d) $\mathrm{Nm}((L \cap L')^*) = \mathrm{Nm}(L^*) \cdot \mathrm{Nm}(L'^*)$

(e) Every subgroup of K^* containing a norm group is itself a norm group.

Lemma 1.1.7. Let L be an extension of K. If $\mathrm{Nm}(L^*)$ is of finite index in K^*, then it is open.

Proof. We first show that $\mathcal{O}_K$ is compact. Recall that a metric space is compact if and only if it is complete and totally bounded. The completeness of $\mathcal{O}_K$ is from the definition. Note that any element in $\mathcal{O}_K$ has the form

$$a = s_0 + s_1\pi + \cdots + s_n\pi^n + \cdots$$

there are finite elements

$$s_0 + s_1\pi + \cdots + s_n\pi^n$$

such that a is within $|\pi^{n+1}|$ of such an element. Therefore $\mathcal{O}_K$ is totally bounded and then is compact.

As a closed subset of $\mathcal{O}_K$, $\mathcal{O}_K^*$ is also compact. Similarly $\mathcal{O}_L^*$ is compact in L. Then $\mathrm{Nm}(\mathcal{O}_L^*)$ is a compact subgroup of K^* and hence a closed subgroup of $\mathcal{O}_K^*$. One can check that

$$\mathrm{Nm}(L^*) \cap \mathcal{O}_K^* = \mathrm{Nm}(\mathcal{O}_L^*)$$

Then there is a natural injective homomorphism

$$\mathcal{O}_K^*/\mathrm{Nm}(\mathcal{O}_L^*) \hookrightarrow K^*/\mathrm{Nm}(L^*)$$

Thus $\mathrm{Nm}(\mathcal{O}_L^*)$ is closed of finite index in $\mathcal{O}_K^*$, it is then an open subgroup of $\mathcal{O}_K^*$. Note that $\mathcal{O}_K^*$ itself is a open subgroup of K^* (since the valuation $|\cdot|$ is discrete and then we may choose ϵ such that $\mathcal{O}_K^* = \bigcup_{x \in \mathcal{O}_K^*} \{y : |y - x| < \epsilon\}$), $\mathrm{Nm}(\mathcal{O}_L^*)$ is open in K^*. Therefore, $\mathrm{Nm}(L^*)$ is a subgroup containing an open subgroup, hence is open as the union of open cosets. ■

Theorem 1.1.8 (Local Existence Theorem)**.** The norm groups (the set of the subgroups like $\mathrm{Nm}(L^*)$ for finite Abelian extension L) in K^* are exactly the open subgroups of finite index.

Remark 1.1.9. *If K has characteristic 0, every subgroup $H \subseteq K^*$ of finite index is open, but this is not true for K with characteristic $p > 0$.*

Remark 1.1.10. *If L/K is a finite Abelian extension with conductor 0, that is, $\mathcal{O}_K^* \subseteq \mathrm{Nm}(L^*)$. Since $\mathrm{Nm}(L^*)$ has finite index in K^*, there exists a minimal number n such that $\pi^n \in \mathrm{Nm}(L^*)$, it is not hard to check that in this case $\mathrm{Nm}(L^*) = \bigcup_{k\in\mathbb{Z}} \mathcal{O}_K^* \pi^{kn}$. Consider the n-dimensional unramified extension L'/K, its norm group $\mathrm{Nm}(L'^*)$ is also the group $\bigcup_{k\in\mathbb{Z}} \mathcal{O}_K^* \pi^{kn}$, then $\mathrm{Nm}(L'^*) = \mathrm{Nm}(L^*)$, which implies $L = L'$.*

1.1.1 Outline of the proofs of the main theorems

Theorem 1.1.11. The mapping ϕ_K described in the "Local Reciprocity Law" is unique.

Proof. If the mapping ϕ_K exists and the "Local Existence Theorem" holds, let π be a prime element of $\mathcal{O}_K$ and we may choose a field $K_{\pi,n}$ such that $\mathrm{Nm}(K_{\pi,n}) = (1+\mathfrak{m}^n)\langle\pi\rangle$, then the field $K_\pi = \bigcup_{n\geq 1} K_{pi,n}$. Note that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$, and $\phi_K(\pi)$ acts K^{un} as Frob_K, the action of $\phi_K(\pi)$ on K^{ab} is determined. Hence $\phi(\pi) = \phi'(\pi)$ for any two mapping ϕ, ϕ' satisfying the conditions and any π. Note that $\{\pi : \pi \text{ is a prime element}\}$ generates the whole multiplicative group K^*, we obtain that $\phi = \phi'$. ■

For the existence of ϕ_K and the proof of the "Local Existence Theorem", we will give sketches of three proofs, which will be filled up in the following sections.

Sketch of proof I: from Lubin-Tate and Hasse-Arf. The theory of Lubin and Tate constructs the fields $K_{\pi,n}$ for each π, and thus we obtain the structure of K_π. And the theory also provides the homomorphism $\phi_\pi : \mathcal{O}_K^* \to \mathrm{Gal}(K_\pi/K)$. Moreover, it shows that it can be uniquely extended to $K^* \to \mathrm{Gal}(K_\pi \cdot K^{\mathrm{un}}/K)$ such that $\phi(\pi)|_{K^{\mathrm{un}}} = \mathrm{Frob}_K$ are independent of π.

We can check that the conclusion holds for $K_\pi \cdot K^{\mathrm{un}}$, thus it remains to show that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. This follows from the Hasse-Arf theorem. ■

Sketch of proof II: from Lubin-Tate and Cohomology. ■

Sketch of proof III: using Cohomology and Hilbert symbol. ■

2 The Cohomology of Groups

2.1 Cohomology

Definition 2.1.1. Let $H \subseteq G$ be groups. For an H-module M, define Ind_H^G to be the set of maps (not necessarily homomorphisms) $\varphi : G \to M$ such that $\varphi(hg) = h\varphi(g)$ for all $h \in G$. Then $\mathrm{Ind}_H^G(M)$ becomes a G-module with $(g\varphi)(x) = \varphi(xg)$. A homomorphism $\alpha : M \to M'$ induces a homomorphism

$$\varphi \mapsto \alpha \circ \varphi : \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M')$$

Remark 2.1.2. *The category of G-modules can be identified with the category of the $\mathbb{Z}[G]$-modules*

Lemma 2.1.3. (a) We have $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M, N)$

(b) The functor Ind_H^G is exact.

(c) Let ϕ be the natural map

$$\phi : \mathrm{Ind}_H^G(N) \to N$$
$$\varphi \mapsto \varphi(1)$$

this is an H-homomorphism. Then any H-homomorphism $M \to N$ can be lifting to a G-homomorphism $M \to \mathrm{Ind}_H^G(N)$.

Definition 2.1.4. If $H = \{1\}$, an H-module is just an Abelian group. Thus $\mathrm{Ind}_H^G(M) = \{\varphi : G \to M\} = \mathrm{Hom}(\mathbb{Z}[G], M)$. A G-module is said to be induced if it is isomorphic to this for some Abelian group M.

Proposition 2.1.5. The category of G-modules has enough injectives. Indeed, for any injective element I in the category of Abelian groups, $\mathrm{Ind}^G(I)$ is injective as G-modules.

Definition 2.1.6. Let M be a G-module, and choose an injective resolution

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} \to \cdots$$

Then it induces a complex

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \to \cdots$$

Define the rth cohomology group of G with coefficients in M to be

$$H^r(G, M) = \mathrm{Ker}(d^r)/\mathrm{Im}(d^{r-1})$$

Proposition 2.1.7. We have $H^0(G, M) = M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$, where $\mathbb{Z}$ is treated as a trivial G-module.

Proposition 2.1.8. If M is injective, then for $r > 0$ we have $H^r(G, M) = 0$.

Proposition 2.1.9 (Shapiro's lemma)**.** Let H be a subgroup of G. For every H-module N, there is a canonical isomorphism

$$H^r(G, \mathrm{Ind}_H^G(N)) \to H^r(H, N)$$

for all $r \geq 0$.

Corollary 2.1.10. If M is an induced G-module, then $H^r(G, M) \cong H^r(\{1\}, M_0) = 0$ for all $r > 0$.

Definition 2.1.11. Let $P_r, r \geq 0$ be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, \cdots, g_r)$ of elements of G, endow the action of G such that

$$g(g_0, \cdots, g_r) = (gg_0, \cdots, gg_r)$$

Note that P_r is also free as a $\mathbb{Z}[G]$-module, with basis $\{(1, g_1, \cdots, g_r) | g_i \in G\}$. Define a homomorphism

$$d_r : P_r \to P_{r-1}$$

$$(g_0, \cdots, g_r) \mapsto \sum_{i=0}^{r} (-1)^i (g_0, \cdots, \hat{g}_i, \cdots, g_r)$$

Then (P_r, d_r) defines a complex

$$\cdots P_r \xrightarrow{d_r} P_{r-1} \to \cdots \to P_0$$

Let $\epsilon : P_0 \to \mathbb{Z}$ be the map sending every basis element (g_0) to 1.

Proposition 2.1.12. The complex

$$P_\bullet \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is exact.

Proposition 2.1.13. $P_\bullet$ is actually a projective resolution of $\mathbb{Z}$, then we have

$$H^r(G,M)\cong H^r(\mathrm{Hom}_G(P_\bullet,M))$$

Remark 2.1.14. *Note that the elements in* $\mathrm{Hom}_G(P_r,M)$ *can be identified with functions* $\varphi: G^{r+1}\to M$ *fixed by* G*, i.e.,*

$$\varphi(gg_0,\cdots,gg_r)=g(\varphi(g_0,\cdots,g_r))$$

Thus $\mathrm{Hom}_G(P_r,M)$ *can be identified with the set* $\tilde{C}^r(G,M)$ *of* φ*'s satisfying this condition. Such* φ *are called homogeneous* r*-cochains of* G *with values in* M*. The boundary map* $\tilde{d}^r:\tilde{C}^r(G,M)\to\tilde{C}^{r+1}(G,M)$ *induced by* d^{r+1} *is*

$$(\tilde{d}^r\varphi)(g_0,\cdots,g_{r+1})=\sum(-1)^i\varphi(g_0,\cdots,\hat{g}_i,\cdots,g_{r+1})$$

Then the proposition above says that

$$H^r(G,M)\cong\mathrm{Ker}(\tilde{d}^r)/\mathrm{Im}(\tilde{d}^{r-1})$$

Let $C^r(G,M)$ *be the group of inhomogeneous* r*-cochains of* G *with values in* M *consisting of all maps* $\varphi:G^r\to M$*. Set* $G^0=\{1\}$ *and hence* $C^0(G,M)=M$*. Define*

$$d^r:C^r(G,M)\to C^{r+1}(G,M)$$

by

$$(d^r\varphi)(g_1,\cdots,g_{r+1})=g_1\varphi(g_2,\cdots,g_{r+1})+\sum_{j=1}^{r}(-1)^j\varphi(g_1,\cdots,g_jg_{j+1},\cdots,g_{r+1})+(-1)^{r+1}\varphi(g_1,\cdots,g_r)$$

Define

$$Z^r(G,M)=\mathrm{Ker}(d^r)$$
$$B^r(G,M)=\mathrm{Im}(d^{r-1})$$

Note that for $\varphi\in\tilde{C}^r(G,M)$*, it only depends on the values of* $(1,g_0^{-1}g_1,\cdots,g_0^{-1}g_r)$*, or equivalently,* φ *can one-to-one correspond to a function on the set* $\{(g_1,g_1g_2,\cdots,g_1\cdots g_r)|g_i\in G\}$*. If we make the coordinate transformation*

$$\varphi'(g_1,\cdots,g_r)=\varphi(1,g_1,g_1g_2,\cdots,g_1\cdots g_r)$$

we obtain an element $\varphi'\in C^r(G,M)$*. And we have*

$$(d^r\varphi')(g_1,\cdots,g_{r+1})=g_1\varphi'(g_2,\cdots,g_{r+1})+\sum_{j=1}^{r}(-1)^j\varphi'(g_1,\cdots,g_jg_{j+1},\cdots,g_{r+1})+(-1)^{r+1}\varphi'(g_1,\cdots,g_r)$$
$$=g_1\varphi(1,g_2,g_2g_3,\cdots,g_2\cdots g_{r+1})+\sum_{j=1}^{r}(-1)^j\varphi(1,g_1,\cdots,g_1\cdots g_{j-1},g_1\cdots g_jg_{j+1},\cdots,g_1\cdots g_{r+1})$$
$$+(-1)^{r+1}\varphi(1,g_1,g_1g_2,\cdots,g_1\cdots g_r)$$
$$=(\tilde{d}^r\varphi)'(g_1,\cdots,g_{r+1})$$

Therefore, we build a bijection between (C^r,d^r) *and* $(\tilde{C}^r,\tilde{d}^r)$*, and then*

$$H^r(G,M)\cong Z^r(G,M)/B^r(G,M)$$

Example 1. We use the remark above to compute $H^1 = Z^1/B^1$. Compute that

$$B^1(G,M) = \mathrm{Im}(M = C^0(G,M) \xrightarrow{d^0} C^1(G,M)) = \{\varphi : G \to M | \varphi(g) = gm - m \text{ for some } m \in M\}$$

$$Z^1(G,M) = \{\varphi : G \to M | g_1\varphi(g_2) + \varphi(g_1) = \varphi(g_1g_2)\}$$

We call the elements in $Z^1(G,M)$ the crossed homomorphism and the elements in $B^1(G,M)$ the principal crossed homomorphism.

In particular, if the action of G on M is trivial, i.e., $gm = m$. Then $B^1 = \{0\}$ and $Z^1 = \mathrm{Hom}(G,M)$.

In particular, if G is generated by a single element σ, let φ be a crossed homomorphism. Note that

$$\varphi(\sigma^2) = \sigma\varphi(\sigma) + \varphi(\sigma)$$

$$\varphi(\sigma^3) = \sigma^2\varphi(\sigma) + \sigma\varphi(\sigma) + \varphi(\sigma)$$

$$\cdots\cdots$$

Define a map $\mathrm{Nm}_G : M \to M$ via $m \mapsto \sum_\sigma \sigma m$, then $H^1(G,M) \cong \mathrm{Ker}(\mathrm{Nm}_G)/(\sigma - 1)M$.

Proposition 2.1.15. If L is a finite Galois extension of a field K, let $G = \mathrm{Gal}(L/K)$, then L and L^* become G-modules. We have $H^1(G, L^*) = 0$.

Proof. The group $Z^1(G,L^*)$ consists of all maps $\varphi : G \to L^*$ such that $\varphi(\sigma_2)^{\sigma_1} \cdot \varphi(\sigma_1) = \varphi(\sigma_1\sigma_2)$, where $\sigma_i \in G$. Fix an element $a \in L^*$, and let $b = \sum_{\sigma\in G} \varphi(\sigma)a^\sigma$. We first suppose that $b \neq 0$. Then $b^\tau = \sum_\sigma \varphi(\sigma)^\tau \cdot a^{(\tau\sigma)}$. Compute that

$$\varphi(\tau)\tau b = \sum_\sigma \varphi(\tau)\varphi(\sigma)^\tau \cdot a^{(\tau\sigma)} = \sum_\sigma \varphi(\tau\sigma) \cdot a^{(\tau\sigma)} = b$$

That is, $\varphi(\tau) = b/\tau b$. Then φ is in $B^1(G,L^*)$.

It remains to show that there exists an element a for which $b \neq 0$. Indeed, if $\sum_\sigma \varphi(\sigma)\sigma$ is a zero map, by Artin theorem (see https://math.stackexchange.com/questions/2082648/proof-of-artins-theorem-linearly-independent-functions) every $\varphi(\sigma)$ is 0. ■

Corollary 2.1.16. Let L/K be a cyclic extension, and let σ generate $\mathrm{Gal}(L/K)$. If $\mathrm{Nm}_{L/K}a = 1$, then a is of the form $\sigma b/b$.

Proposition 2.1.17. With the same hypothesis above, we have $H^r(G,L) = 0$ for all $r > 0$.

Proof. Choose an element α such that $\{\sigma\alpha : \sigma \in \mathrm{Gal}(L/K)\}$ forms a normal basis of L/K (see https://en.wikipedia.org/wiki/Normal_basis). Thus there exists an isomorphism of G-modules

$$\sum_{\sigma\in G} a_\sigma\sigma \mapsto \sum_{\sigma\in G} a_\sigma\sigma\alpha : K[G] \to L$$

But $K[G] = \mathrm{Ind}_1^G K$, thus $H^r(G,L) \cong H^r(1,K) = 0$ for $r > 0$. ■

Definition 2.1.18. Let M and M' respectively be G and G'-modules. Homomorphisms

$$\alpha : G' \to G, \quad \beta : M \to M'$$

are said to be compatible if

$$\beta(\alpha(g)m) = g(\beta(m))$$

Then α and β induce a homomorphism of complexes

$$C^\bullet(G, M) \to C^\bullet(G', M'), \quad \varphi \mapsto \beta \circ \varphi \circ \alpha^r$$

and hence homomorphisms

$$H^r(G, M) \to H^r(G', M')$$

Example 2. (a) Let H be a subgroup of G. For every H-module M, the map

$$\varphi \mapsto \varphi(1_G) : \mathrm{Ind}_H^G(M) \to M$$

is compatible with the inclusion $H \hookrightarrow G$, and the induced homomorphism

$$H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(H, M)$$

is the isomorphism in Shapiro's lemma.

(b) Let α be the inclusion $H \hookrightarrow G$ and let β be the identify map on a G-module M. In this case we obtain the restriction homomorphisms

$$\mathrm{Res} : H^r(G, M) \to H^r(H, M)$$

They can also be constructed as follows: let $M \to \mathrm{Ind}_H^G(M)$ be the homomorphism sending m to the map $g \mapsto gm$, then the composition

$$H^r(G, M) \to H^r(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H^r(H, M)$$

is exactly the restriction map.

(c) Let H be a normal subgroup of G and α the quotient map $G \to G/H$. Let β be the inclusion $M^H \hookrightarrow M$. In this case, we obtain the inflation homomorphisms

$$H^r(G/H, M^H) \to H^r(G, M)$$

(d)

(e) Let H be a subgroup of finite index of G, and let S be a set of left coset representatives for H in G, $G = \bigcup_{s \in S} sH$. Let M be a G-module. For any $m \in M^H$, $\mathrm{Nm}_{G/H} m \triangleq \sum_{s \in S} sm$ is independent of the choice of S, and is fixed by G. Thus we actually obtain a homomorphism $\mathrm{Nm}_{G/H} : M^H \to M^G$. This can be extended to a corestriction homomorphism

$$\mathrm{Cor} : H^r(H, M) \to H^r(G, M)$$

as follows: there is a canonical homomorphism of G-modules

$$\varphi \mapsto \sum_{s \in S} s\varphi(s^{-1}) : \mathrm{Ind}_H^G M \to M$$

and hence

$$H^r(H, M) \xrightarrow{\sim} H^r(G, \mathrm{Ind}_H^G M) \to H^r(G, M)$$

Proposition 2.1.19. Let H be a subgroup of G of finite index. The composite

$$\mathrm{Cor} \circ \mathrm{Res} : H^r(G, M) \to H^r(G, M)$$

is multiplication by $(G : H)$.

Corollary 2.1.20. If $(G : 1) = m$, then $mH^r(G, M) = 0$ for all $r > 0$.

Corollary 2.1.21. If G is finite and M is finitely generated as an Abelian group, then $H^r(G, M)$ is finite.

Proof. This is a finitely-generated group killed by $|G|$, thus, it is a finite group. ■

Corollary 2.1.22. We call the p-primary component of a Abelian group A the subgroup consisting of all elements killed by a power of p. Let G be a finite group and G_p its Sylow p-subgroup. For every G-module M, the restriction map

$$\mathrm{Res} : H^r(G, M) \to H^r(G_p, M)$$

is injective on the p-primary component of $H^r(G, M)$.

Proposition 2.1.23. Let H be a normal subgroup of G, and let M be a G-module. Let r be a positive integer. If $H^j(H, M) = 0$ for all j with $0 < j < r$, then the sequence

$$0 \to H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(H, M)$$

is exact.

Proof. First we consider the case $r = 1$.

Obviously, the inflation map is an injection. For the second part, choose a $\varphi \in H^1(G, M)$ with $\varphi|_H = hm_0 - m_0$. Define $\varphi'(g) = \varphi(g) - (hm_0 - m_0)$. Then $\varphi' = \varphi$ in $H^1(G, M)$ and $\varphi'(H) = 0$.

Now we prove that φ' takes values in M^H. Recall that we have

$$\varphi'(hg) = h\varphi'(g) + \varphi'(h) = h\varphi'(g)$$

$$\varphi'(gh') = g\varphi'(h') + \varphi'(g) = \varphi'(g)$$

Since H is normal in G, we can make $hg = gh'$. Thus, $h\varphi'(g) = \varphi'(g)$.

Now we prove by induction on r.

In fact, let $M_1 = \mathrm{Ind}_1^G(M_0)/M$, where M_0 here is M regarded as an Abelian group, we have

$$H^{r-1}(G, M_1) \cong H^r(G, M)$$

Then we can reduce the case r to the case $r - 1$. ■

Corollary 2.1.24. If $\Omega \supseteq L$ are Galois extensions of K, then $H \triangleq \mathrm{Gal}(\Omega/L)$ is a normal subgroup of $G = \mathrm{Gal}(\Omega/K)$. Recall that $H^1(H, \Omega^*) = 0$, thus there is an exact sequence

$$0 \to H^2(G/H, L^*) \to H^2(G, \Omega^*) \to H^2(H, \Omega^*)$$

Proposition 2.1.25. There exists one and only one family of bi-additive pairings

$$(m,n)\mapsto m\cup n : H^r(G,M)\times H^s(G,N)\to H^{r+s}(G,M\otimes N)$$

defined for all G-modules M, N and all integers $r,s\geq 0$, satisfying the following conditions:

(a) these maps become morphisms of functors when the two sides are regarded as covariant bifunctors on (M,N)

(b) for $r=s=0$, the pairing is

$$(m,n)\mapsto M\otimes n : M^G\otimes N^G\to (M\otimes N)^G$$

(c) if $0\to M'\to M\to M''\to 0$ is an exact sequence of G-modules such that

$$0\to M'\otimes N\to M\otimes N\to M''\otimes N\to 0$$

is exact, then

$$(\delta m'')\cup n=\delta(m''\cup n),\quad m''\in H^r(G,M''),\ n\in H^s(G,N)$$

Here δ denotes the connecting homomorphism $H^r(G,M'')\to H^{r+1}(G,M')$ or $H^{r+s}(G,M''\otimes N)\to H^{r+s+1}(G,M'\otimes N)$.

(d) if $0\to N'\to N\to N''\to 0$ is an exact sequence of G-modules such that

$$0\to M\otimes N'\to M\otimes N\to M\otimes N''\to 0$$

is exact, then

$$m\cup\delta n''=(-1)^r\delta(m\cup n''),\quad m\in H^r(G,M),\ n''\in H^s(G,N'')$$

Proposition 2.1.26. (a) $(x\cup y)\cup z=x\cup(y\cup z)$

(b) $x\cup y=(-1)^{rs}y\cup x$

(c) $\mathrm{Res}(x\cup y)=\mathrm{Res}(x)\cup\mathrm{Res}(y)$

(d) $\mathrm{Cor}(x\cup\mathrm{Res}y)=\mathrm{Cor}(x)\cup y$

(e) $\mathrm{Inf}(x\cup y)=\mathrm{Inf}(x)\cup\mathrm{Inf}(y)$.

2.2 Homology

Definition 2.2.1. For a G-module M, let M_G be the quotient of M by the subgroup I_M generated by $\{gm-m|g\in G,m\in M\}$.

Proposition 2.2.2. The functor $M\mapsto M_G$ is right exact.

Proof. Assume that $0\to M'\xrightarrow{\phi}M\xrightarrow{\varphi}M''\xrightarrow{\psi}0$ is exact.

If $\bar{b}\in\mathrm{Ker}(M_G\to M''_G)$, that is, $\varphi(b)\in I_{M''}$. Note that $\varphi(I_M)=\varphi(I_{M''})$, then $\varphi(b-b')=0$ for some $b'\in I_M$. Then $b-b'\in\mathrm{Ker}(\varphi)=\mathrm{Im}(\phi)$. Suppose $\phi(a)=b-b'$. Thus $\bar{a}\mapsto\bar{b}$, i.e., $\mathrm{Ker}(M_G\to M''_G)=\mathrm{Im}(M'_G\to M_G)$.

For any $\bar{c}\in M''_G$, set $\varphi(b)=c$. Then $\bar{b}\mapsto\bar{c}$. Therefore, $M'_G\to M_G\to M''_G\to 0$ is exact. ■

Definition 2.2.3. Let M be a G-module, and choose a projective resolution

$$\cdots P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

of M. The homology group of

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \to 0$$

is $H^r(G, M) = \mathrm{Ker}(d_r)/\mathrm{Im}(d_{r+1})$ is called the homology of M.

Proposition 2.2.4. (a) $H_0(G, P) = M_G$

(b) If P is a projective G-module, then $H_r(G, P) = 0$ for all $r > 0$.

Proposition 2.2.5. There is a canonical isomorphism

$$H_1(G, \mathbb{Z}) \cong G^{ab} = G/[G, G]$$

Proof. Define the augmentation map

$$\mathbb{Z}[G] \to \mathbb{Z}, \quad \sum n_g g \mapsto \sum n_g$$

Its kernel is called the augmentation ideal I_G. Clearly I_G is a free $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ with basis $\{g - 1 | g \in G, g \neq 1\}$, and so

$$M/I_G M = M_G \cong H_0(G, M)$$

Consider the exact sequence

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

Since the G-module $\mathbb{Z}[G]$ is projective, and so $H_1(G, \mathbb{Z}[G]) = 0$. Therefore we obtain an exact sequence

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G \to \mathbb{Z} \to 0$$

Note that the middle map $I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ is zero, then we have

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

and

$$\mathbb{Z}[G]_G = \mathbb{Z}[G]/I_G \cong \mathbb{Z}$$

Consider the map

$$G/[G, G] \to I_G/I_G^2, \quad g + [G, G] \mapsto g - 1 + I_G^2$$

this is well-defined since $ab - 1 = a + b - 2 = ba - 1$ in I_G/I_G^2. To show this is an isomorphism, we may construct its converse. There is a natural homomorphism

$$I_G \to G^{ab}, \quad g - 1 \mapsto g + [G, G]$$

Then it is obvious that the generators of I_G^2, $(g - 1)(g' - 1)$ sends to 1. Therefore it induces the inverse

$$I_G/I_G^2 \to G^{ab}$$

Hence

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

■

2.3 The Tate group

Definition 2.3.1. For a G-module M, the norm map $\mathrm{Nm}_G : M \to M$ is defined to be

$$m \mapsto \sum_{g\in G} gm$$

We have $\mathrm{Im}(\mathrm{Nm}_G) \subseteq M^G$ and $I_G M \subseteq \mathrm{Ker}(\mathrm{Nm}_G)$. Therefore, the homomorphism

$$M \xrightarrow{\mathrm{Nm}_G} M$$

induces a natural homomorphism

$$H_0(G, M) = M/I_G M \xrightarrow{\mathrm{Nm}_G} H^0(G, M) = M^G$$

By computing its kernel and image we obtain an exact sequence

$$0 \to \mathrm{Ker}(\mathrm{Nm}_G)/I_G M \to H_0(G, M) \xrightarrow{\mathrm{Nm}_G} H^0(G, M) \to M^G/\mathrm{Nm}_G(M) \to 0$$

Define the Tate cohomology group

$$\hat{H}^r(G, M) = H_T^r(G, M) = \begin{cases} H^r(G, M), & r > 0 \\ M^G/\mathrm{Nm}_G(M), & r = 0 \\ \mathrm{Ker}(\mathrm{Nm}_G)/I_G M, & r = -1 \\ H_{-r-1}(G, M), & r < -1 \end{cases}$$

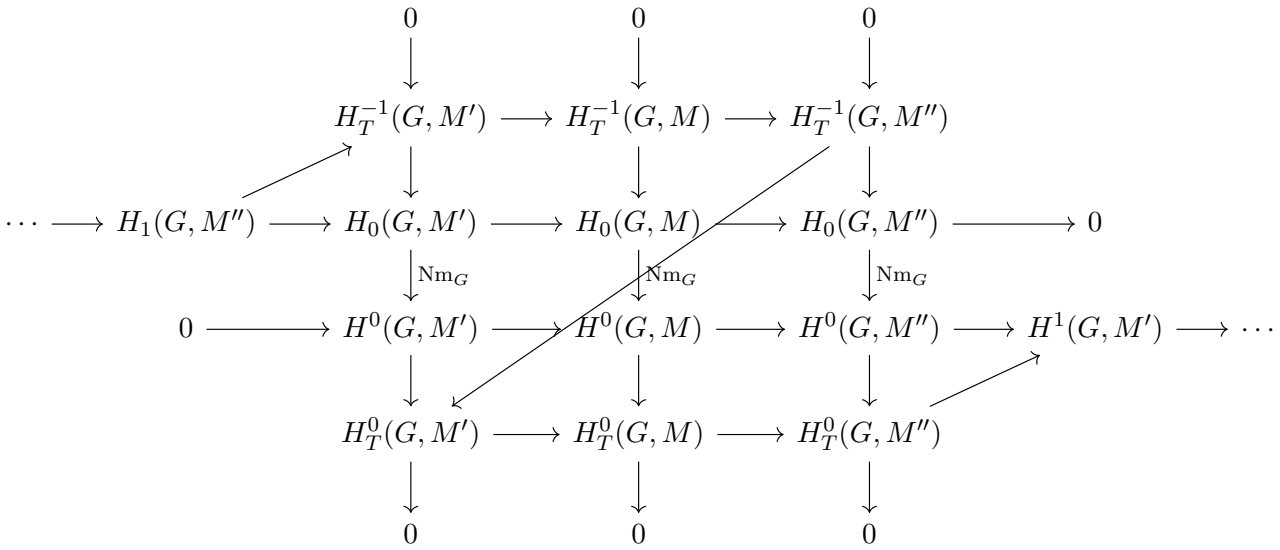
Thus the sequence above becomes

$$0 \to H_T^{-1}(G, M) \to H_0(G, M) \xrightarrow{\mathrm{Nm}_G} H^0(G, M) \to H_T^0(G, M) \to 0$$

Proposition 2.3.2. For any exact sequence of G-modules, we have a diagram

$$\begin{array}{ccccccccccc}
 & & & & 0 & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & H_T^{-1}(G,M') & \longrightarrow & H_T^{-1}(G,M) & \longrightarrow & H_T^{-1}(G,M'') & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H_1(G,M'') & \longrightarrow & H_0(G,M') & \longrightarrow & H_0(G,M) & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \\
0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M'') & \longrightarrow & H^1(G,M') & \longrightarrow & \cdots \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & H_T^0(G,M') & \longrightarrow & H_T^0(G,M) & \longrightarrow & H_T^0(G,M'') & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & & 0 & &
\end{array}$$

Note that the composition $H_1(G, M) \to H_0(G, M') \to H^0(G, M')$ is the zero map, then the image of $H_1(G, M)$ is contained in $H_T^{-1}(G, M')$. By snake lemma we have a new diagram



Thus we obtain a long exact sequence

$$\cdots \to H_T^r(G,M') \to H_T^r(G,M) \to H_T^r(G,M'') \to H_T^{r-1}(M') \to \cdots$$

Proposition 2.3.3. If M is induced, then $H_T^r(G,M) = 0$ for all $r \in \mathbb{Z}$.

Proposition 2.3.4. The functors $\mathrm{Cor}, \mathrm{Res}$ can be uniquely extended to the Tate groups. The cup product can also extend uniquely.

Corollary 2.3.5. The Tate group $H_T^r(G,M)$ is killed by $|G|$ for all r.

Now we turn to the cohomology of finite cyclic group.

Lemma 2.3.6. For every finite group G

(a) $H_T^r(G,\mathbb{Q}) = 0$ for all $r \in \mathbb{Z}$

(b) $H_T^0(G,\mathbb{Z}) = \mathbb{Z}/(G:1)\mathbb{Z}$ and $H^1(G,\mathbb{Z}) = 0$

(c) there is a canonical isomorphism

$$\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G,\mathbb{Z})$$

Proof. (a) Since H_T^r is killed by $|G|$, and note that $\times m : H_T^r(G,\mathbb{Q}) \to 0 \hookrightarrow H_T^r(G,\mathbb{Q})$ can also be induced from the isomorphism $\times m : \mathbb{Q} \to \mathbb{Q}$, we have $H_r^T(G,\mathbb{Q})$ is exactly 0.

(b) We have $H_T^0(G,\mathbb{Z}) = \mathbb{Z}^G = \mathbb{Z}$, and the norm map is multiplication by $|G|$. Hence $H_T^0(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$. Moreover, $H_T^1(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Z}) = 0$.

(c) The exact sequence

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

induces that

$$0 = H^1(G,\mathbb{Q}) \to \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z}) \to 0 = H^2(G,\mathbb{Q})$$

Then the isomorphism follows immediately. ∎

Proposition 2.3.7. Let $G = \langle \sigma \rangle$ be a finite cyclic group. Then there is an isomorphism

$$H_T^r(G, M) \xrightarrow{\sim} H_T^{r+2}(G, M)$$

Proof. There is an exact sequence

$$0 \to \mathbb{Z} \xrightarrow{m \mapsto \sum_{g \in G} gm} \mathbb{Z}[G] \xrightarrow{\sigma - 1} \mathbb{Z}[G] \xrightarrow{\sigma \mapsto 1} \mathbb{Z} \to 0$$

Since every term and kernel is a free module, then it remains exact as G-modules after tensoring with M

$$0 \to M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes M \to M \to 0$$

Since $\mathbb{Z}[G] \otimes M$ is just the induced module $\mathrm{Ind}^G(M)$, $H_T^r(G, \mathbb{Z}[G] \otimes M) = 0$. Thus by splitting the sequence into two short exact sequences and analyzing their induced long exact sequences we have

$$H_T^r(G, M) \xrightarrow{\sim} H^{r+2}(G, M)$$

■

Definition 2.3.8. Let G be a finite cyclic group. If $H^r(G, M)$ are finite, defined the Herbrand quotient of M to be

$$h(M) = \frac{|H_T^0(G, M)|}{|H_T^1(G, M)|}$$

Lemma 2.3.9. Let $0 \to A_0 \to A_1 \to \cdots \to 0$ be a exact sequence of finite group, then

$$\frac{|A_0||A_2| \cdots}{|A_1||A_3| \cdots} = 1$$

Proof. Break it into short exact sequences. ■

Proposition 2.3.10. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of G-modules. If any two of $h(M'), h(M), h(M'')$ are defined, then so is the third. Moreover,

$$h(M) = h(M')h(M'')$$

Proof. We can construct a long exact sequence as

$$0 \to K \to H_T^0(M') \to H_T^0(M) \to H_T^0(M'') \to H_T^1(M') \to H_T^1(M) \to H_T^1(M'') \to K' \to 0$$

where $K = \mathrm{Coker}(H_T^{-1}(M) \to H_T^{-1}(M''))$ and $K' = \mathrm{Coker}(H_T^1(M) \to H_T^1(M'')) \cong K$. Then the result follows from the lemma above. ■

Proposition 2.3.11. If M is a G-module with finite elements, then $h(M) = 1$.

Proof. There are two exact sequences

$$0 \to H_T^{-1}(M) \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to H_T^0(M) \to 0$$

$$0 \to M^G \to M \xrightarrow{g-1} M \to M_G \to 0$$

where g is any generator of G. Then it can be checked that H_T^{-1} and H_T^0 have the same order. ■

Corollary 2.3.12. Let $\alpha : M \to N$ be a homomorphism of G-modules with finite kernel and cokernel. If either $h(M)$ or $h(N)$ is finite, then so is the other, and they are equal.

Now we can introduce the Tate's theorem

Theorem 2.3.13. Let G be a finite group, and let M be a G-module. If

$$H_T^1(H, M) = 0 = H_T^2(H, M)$$

for all subgroups H of G, then $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$.

Proof. If G is cyclic, then it is obvious.

If G is solvable, we shall prove this theorem by induction on the order of G.

Since G is solvable, it contains a normal subgroup H such that G/H is cyclic. By the inductive hypothesis, $H^r(H, G) = 0$ for all r. By 2.1.23 we have exact sequence for every $r \geq 1$

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M)$$

and thus $H^r(G, M) \cong H^r(G/H, M^H) = 0$ for all $r \geq 1$.

Next we show that $H_T^0(G, M) = 0$. Let $x \in M^G$. Since $H_T^0(G/H, M^H) = 0$, then every element in M^H is in the image of $\mathrm{Nm}_{G/H} M^H$. In particular, $x = \mathrm{Nm}_{G/H} y$ for some $y \in M^H$. By the inductive hypothesis, $H_T^0(H, M) = 0$, there exists $z \in M$ such that $\mathrm{Nm}_H z = y$. Hence $\mathrm{Nm}_G(z) = x$. This implies that $x \in \mathrm{Nm}_G(M)$. Therefore, $H_T^0(G, M) = 0$.

Recall the exact sequence

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

By tensoring M we have a new exact sequence

$$0 \to M' \to \mathrm{Ind}^G(M) \to M \to 0$$

Since the middle term is induced, $H_T^r(H, M) \cong H_T^{r+1}(H, M')$ for all r and all subgroups $H \subseteq G$. In particular, M' satisfies the assumption. By the inductive hypothesis and what we proved above, $H_T^r(G, M) = 0$ $(r \geq -1)$. Repeat these operations, we obtain that $H_T^r(G, M) = 0$ for all r.

For the general case, G_p is solvable for any prime p. Therefore, the result holds true for G. ■

Theorem 2.3.14 (Tate)**.** Let G be a finite group and let C be a G-module. Suppose that for all subgroups H of G

(a) $H^1(H, C) = 0$, and

(b) $H^2(H, C)$ is a cyclic group of order equal to $(H : 1)$

Then, for all r, there is an isomorphism

$$H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, C)$$

depending only on the choice of a generator of $H^2(G, C)$.

Proof. Choose a generator γ in $H^2(G,C)$. Since $\mathrm{Cor}\circ\mathrm{Res} = |G:H|$, $\mathrm{Res}(\gamma)$ generates $H^2(H,C)$.

Let φ be a cocycle representing the class γ. Let $C(\varphi)$ denote the free Abelian group $\bigoplus_{\sigma\in G-1} Cx_\sigma + C$, where x_σ are free symbols for $\sigma \neq 1$, and we define $x_1 = \varphi(1,1) \in C$.

Now we extend the action of G on C to $C(\varphi)$. Define

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \varphi(\sigma,\tau)$$

This action is well-defined.

Recall that

$$B^2(G,C(\varphi)) = \{\psi : G^2 \to C(\varphi) | \psi(\sigma_1,\sigma_2) = \sigma_1\phi(\sigma_2) - \phi(\sigma_1\sigma_2) + \phi(\sigma_1) \text{ for some } \phi : G \to C(\varphi)\}$$

If we define ϕ as $\phi(\sigma) = x_\sigma$, then $\varphi : G^2 \to C \to C(\varphi)$ can be expressed as

$$\sigma\phi(\sigma_2) - \phi(\sigma_1\sigma_2) + \phi(\sigma_1)$$

Thus, γ vanishes under the mapping

$$H^2(G,C) \to H^2(G,C(\varphi))$$

We shall show that $H^1(H,C(\varphi)) = H^2(H,C(\varphi)) = 0$. Recall that we have an exact sequence

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

Since $\mathbb{Z}[G]$ is induced, we can obtain that

$$H_T^r(H,\mathbb{Z}[G]) = 0$$

for all r. Thus

$$H^1(H,I_G) \cong H_T^0(H,\mathbb{Z}) \cong \mathbb{Z}/|H:1|\mathbb{Z}$$
$$H^2(H,I_G) \cong H^1(H,\mathbb{Z}) = 0$$

Define $\alpha : C(\varphi) \to \mathbb{Z}[G]$ via

$$\alpha(c) = 0,\ \forall c \in C$$
$$\alpha(x_\sigma) = \sigma - 1,\ \forall \sigma \in G\backslash\{1\}$$

Clearly,

$$0 \to C \to C(\varphi) \xrightarrow{\alpha} \mathbb{Z} \to 0$$

is an exact sequence of G-modules. Since $H^1(H,C) = 0$, we have the following long exact sequence

$$0 \to H^1(H,C(\varphi)) \to H^1(H,I_G) \to H^2(H,C) \xrightarrow{\mathrm{Res}(\gamma)\mapsto 0} H^2(H,C(\varphi)) \to 0$$

Considering that $\mathrm{Res}(\gamma)$ generates $H^2(H,C)$, we can find that $H^2(H,C(\varphi))$ is exactly zero.

Finally, by 2.3.13, all $H_T^r(H,C(\varphi))$ are zero. Thus

$$H_T^r(G,\mathbb{Z}) \cong H_T^{r+1}(G,I_G) \cong H_T^{r+2}(G,C)$$

■

Remark 2.3.15. *The map $H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G,C)$ is cup-product with the chosen element γ.*

Definition 2.3.16. For a profinite group G and a discrete G-module M, let $C_c^r(G,M)$ be the set of continuous maps $G^r \to M$ and define d^r as before. We obtain some new cohomology groups $H^r(G,M)$. If H runs through all the open normal subgroups of G, we have

$$H^r(G,M) = \varinjlim H^r(G/H, M^H)$$

If $M = \lim \to M_i$, we have

$$H^r(G,M) = \varinjlim H^r(G,M_i)$$

3 Local Class Field Theory: Cohomology

3.1 The Cohomology of Unramified Extensions

Proposition 3.1.1. If L/K is a finite unramified extension of local field K, then the norm map $\mathrm{Nm}_{L/K} : U_L \to U_K$ is surjective.

Proof. Let $U_L^{(m)} = 1 + \mathfrak{m}_L^m = \{1 + a\pi^m | a \in \mathcal{O}_L\}$, where π is a prime element. Then the maps

$$u \mapsto u \pmod{\mathfrak{m}_L} : U_L \to l^*$$

$$1 + a\pi^m \mapsto a \pmod{\mathfrak{m}_L} : U_L^{(m)} \to l$$

induce the isomorphisms

$$U_L/U_L^{(1)} \xrightarrow{\sim} l^*$$
$$U_L^{(m)}/U_L^{(m+1)} \xrightarrow{\sim} l$$

By 2.1.15 we have $H^1(G,l^*) = 0$, and by 2.3.11 $h(l^*) = 1$. Hence $H_T^0(G,l^*) = H_T^1(G,l^*) = 0$, then $H_T^r(G,l^*) = 0$ holds for all $r \in \mathbb{Z}$. In particular, $0 = (l^*)^G/\mathrm{Nm}_G(l^*) = k^*/\mathrm{Nm}_G(l^*)$. Therefore the norm map $l^* \to k^*$ is surjective.

By 2.1.17 we have $H_T^r(G,l) = 0$ for all $r \in \mathbb{Z}$. In particular, the trace map $l \to k$ is surjective.

Now we go back to the norm map $\mathrm{Nm}_{L/K} : U_L \to U_K$. There are two commutative diagram

$$\begin{array}{ccc} U_L & \longrightarrow & l^* \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{l/k}} \\ U_K & \longrightarrow & k^* \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & l \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{tr}} \\ U_K^{(m)} & \longrightarrow & k \end{array}$$

For any $u \in U_K$, suppose that v is the image of u in K^*. Note that the map $U_L \to l^* \to k^*$ is surjective, then there exists an element $w \in U_L$ such that w is the preimage of v in k^*. Using the commutation, it means $\mathrm{Nm}_{L/K}(w)$ and u have the same image in k^*. Hence $u/\mathrm{Nm}_{L/K}(w) \in U_K^{(1)}$. Proceeding these steps in the right diagram, we obtain a series of elements $w, w_1, \cdots$ such that $w_i \in U_L^{(i)}$ and $u/\mathrm{Nm}(ww_1, \cdots, w_n) \in U_K^{(n+1)}$. Then there exists an element v such that $u/\mathrm{Nm}(v) \in \bigcap U_K^{(i)} = \{1\}$, i.e., u is in the image of $\mathrm{Nm}_{L/K} : U_L \to U_K$. ∎

Proposition 3.1.2. Let K be a local field. If L/K is a finite unramified extension with Galois group G, then

$$H_T^r(G, U_L) = 0, \quad \text{for all } r$$

Proof. The above proposition implies that $H_T^0(G, U_L) = 0$. It remains to show that $H_T^1(G, U_L) = 0$.

Consider the exact sequence

$$0 \to U_L \to L^* \to \mathbb{Z} \to 0$$

the induced long exact sequence is

$$0 \to U_K \to K^* \to \mathbb{Z} \to H^1(G, U_L) \to 0$$

Hence $H^1(G, U_L) = 0$. ■

Corollary 3.1.3. If L/K is an infinite unramified extension with Galois group G, then $H^r(G, U_L) = 0$ for all $r > 0$.

Definition 3.1.4. Now we have $H^r(G, U_L) = 0$ for all unramified extension of K. Then the exact sequence

$$0 \to U_L \to L^* \to \mathbb{Z} \to 0$$

gives that

$$H^2(G, L^*) \xrightarrow{\sim} H^2(G, \mathbb{Z})$$

Recall that $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$, then there is a natural map, called the invariant map, defined by

$$\mathrm{Inv}_{L/K} : H^2(G, L^*) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{continuous}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\mathrm{Frob}_{L/K})} \mathbb{Q}/\mathbb{Z}$$

Theorem 3.1.5. There is an isomorphism

$$\mathrm{Inv}_{K^{\mathrm{un}}/K} : H^2(\mathrm{Gal}(K^{\mathrm{un}}/K), (K^{\mathrm{un}})^*) \to \mathbb{Q}/\mathbb{Z}$$

for every $L \subseteq K$ of finite degree over k,

$$\mathrm{Inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^*) \xrightarrow{\sim} \frac{1}{|L:K|}\mathbb{Z}/\mathbb{Z}$$

Proposition 3.1.6. Let L be a finite extension of K of degree n, and let K^{un} and L^{un} be the largest unramified extensions of K and L. Then the following diagram commutes:

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

Definition 3.1.7. Let L/K be a finite unramified extension. The local fundamental element is the element of $H^2(G, L^*)$ such that $u_{L/K} = \mathrm{Inv}_{L/K}^{-1}(\frac{1}{|L:K|})$. By Tate theorem, $u_{L/K}$ defines an isomorphism

$$H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, L^*)$$

Theorem 3.1.8 (Unramified case)**.** Let $r = -2$, the isomorphism above turns to

$$G \xleftarrow{\sim} K^*/\mathrm{Nm}L^*$$

it is exactly the map $\phi_{L/K}$ respectively in the local reciprocity law.

3.2 The Cohomology of Ramified Extensions

Lemma 3.2.1. If L/K is a Galois extension with $|L:K| = n$, then $H^2(G_{L/K}, L^*)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Proof. 2.1.23 and Hilbert theorem 90 tell us that there is an exact sequence

$$0 \to H^2(G_{L/K}, L^*) \to H^2(G_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*) \to H^2(G_{K^{\mathrm{al}}/L}, (K^{\mathrm{al}})^*)$$

Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(G_{K^{\mathrm{un}}/K}, (K^{\mathrm{un}})^*) & \longrightarrow & H^2(G_{L^{\mathrm{un}}/L}, (L^{\mathrm{un}})^*) \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ 0 & \longrightarrow & H^2(G_{L/K}, L^*) & \longrightarrow & H^2(G_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*) & \xrightarrow{\mathrm{Res}} & H^2(G_{K^{\mathrm{al}}/L}, (L^{\mathrm{al}})^*) \end{array}$$

By 5-lemma the first vertical map is injective. ■

Next we prove that $H^2(G_{L/K}, L^*)$ has order n.

Lemma 3.2.2. Let L be a finite Galois extension of K with Galois group G. Then there exists an open subgroup V of $\mathcal{O}_L$, stable under G, such that $H^r(G, V) = 0$ for all $r > 0$.

Proof. Let $\{x_\tau\}$ be a normal basis for L over K. Also, we require that they are in $\mathcal{O}_L$. Take $V = \sum \mathcal{O}_K x_\tau$. This is a stable subgroup under the action of G. Note that it contains π^m for some m, then it contains $\pi^m \mathcal{O}_L$. Thus V is open since V is the union of cosets of $\pi^m \mathcal{O}_L$. Finally, as G-module, $V \cong \mathcal{O}_K[G] \cong \mathrm{Ind}^G \mathcal{O}_K$. Therefore, $H^r(G, V) = 0$ for all $r > 0$. ■

Lemma 3.2.3. Let L, K, G be as in the last lemma. Then there exists an open subgroup V of $\mathcal{O}_L^*$ stable under G such that $H^r(G, V) = 0$ for all $r > 0$.

Lemma 3.2.4. If L/K is a cyclic extension of degree n; then $h(\mathcal{O}_L^*) = h(L^*) = 1$.

Proof. Let V be an open subgroup of $\mathcal{O}_L^*$ with $H^r(G, V) = 0$ for all r. Because $\mathcal{O}_L^*$ is compact, the quotient $\mathcal{O}_L^*/V$ is finite. Thus $h(\mathcal{O}_L^*) = 1$. Also $h(L^*) = h(\mathcal{O}_L^*)h(\mathbb{Z}) = n$. ■

Theorem 3.2.5. Let L be a finite Galois extension of K with $|L:K| = n$. Then $H^2(G_{L/K}, L^*)$ has order n.

Proof. The ramification filtration gives us that the Galois group $G_{L/K}$ is solvable. Thus we can choose K' such that $L \supseteq K' \supseteq K$. Also there is an exact sequence

$$0 \to H^2(G_{K'/K}, K'^*) \to H^2(G_{L/K}, L^*) \to H^2(G_{L/K'}, L^*)$$

Thus, by reduction on n we can conclude the result. ■

Theorem 3.2.6. For every local field K, there exists a canonical isomorphism

$$\mathrm{Inv}_K : H^2(G_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*) \to \mathbb{Q}/\mathbb{Z}$$

From the same method from 3.2.1, we can obtain an isomorphism

$$\mathrm{Inv}_K : H^2(G_{L/K}, L^*) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

Proof. The diagram in the proof of 3.2.1 becomes

$$\begin{array}{ccccccc}
0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(G_{K^{\mathrm{un}}/K}, (K^{\mathrm{un}})^*) & \longrightarrow & H^2(G_{L^{\mathrm{un}}/L}, (L^{\mathrm{un}})^*) \\
 & & \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\
0 & \longrightarrow & H^2(G_{L/K}, L^*) & \longrightarrow & H^2(G_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*) & \xrightarrow{\mathrm{Res}} & H^2(G_{K^{\mathrm{al}}/L}, (L^{\mathrm{al}})^*)
\end{array}$$

But considering that $H^2(G_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*)$ is exactly the union of all $H^2(G_{L/K}, L^*)$ for any finite Galois extension L/K, we have that the second vertical map is indeed an isomorphism. ■

Definition 3.2.7. Let L be a finite Galois extension of K with Galois group G. We define the fundamental class $u_{L/K} \in H^2(G_{L/K}, L^*)$ to be the element mapping to $\dfrac{1}{|L:K|}$ under $\mathrm{Inv}_{L/K}$.

3.3 The Local Artin Map

Theorem 3.3.1 (general case)**.** For any finite Galois extension of local fields L/K and $r \in \mathbb{Z}$, by Tate theorem, the homomorphism

$$H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^{r+2}(\mathrm{Gal}(L/K), L^*)$$

is an isomorphism. When $r = -2$, it turns to be

$$G^{\mathrm{ab}} \cong K^*/\mathrm{Nm}_{L/K}(L^*)$$

We call its inverse map the local Artin map, denoted by $\phi_{L/K}$.

Proposition 3.3.2. The maps $\phi_{L/K}$ induce the map $\phi_K : K^* \to G = \mathrm{Gal}(K^{\mathrm{al}}/K)$. This map satisfies the conditions of the local reciprocity law.

Theorem 3.3.3 (Norm Limitation Theorem)**.** Suppose L/K is a finite separable extension of non-archimedean local fields and E/K is the maximal abelian sub-extension in L. Then,

$$\mathrm{Nm}_{L/K}(L^*) = \mathrm{Nm}_{E/K}(E^*)$$

This theorem shows that there is no hope of classifying non-Abelian extensions of a local field in terms of the norm groups.

Proof. If L/K is Galois, then $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$. From the local Artin map we can conclude a canonical isomorphism

$$K^*/\mathrm{Nm}_{L/K}(L^*) \cong K^*/\mathrm{Nm}_{L/K}(E^*)$$

However, we know that $\mathrm{Nm}(L^*)$ is a subgroup of $\mathrm{Nm}(E^*)$, thus, they are equal.

In the general case, we assume that L' is the minimal Galois extension of K containing L. Let $G = \mathrm{Gal}(L'/K)$ and $H = \mathrm{Gal}(L'/L)$. The subgroup of G fixing E is $G' \cdot H$, where G' is the derived group of G. Let $a \in \mathrm{Nm}(E^*)$, we have to show that $a \in \mathrm{Nm}(L^*)$. Consider the diagram

$$\begin{array}{ccc} L^* & \xrightarrow{\phi_{L'/L}} & H/H' \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ K* & \xrightarrow{\phi_{L'/K}} & G/G' \\ \| & & \downarrow \\ K^* & \xrightarrow{\phi_{E/K}} & G/G'H \end{array}$$

There exists $b \in L^*$ such that $\phi_{L'/K}(a) = \phi_{L'/K}(\mathrm{Nm}(b))$, and hence $a/\mathrm{Nm}(b) = \mathrm{Nm}(c)$ for some $c \in (L^*)'$. Thus, $a \in \mathrm{Nm}_{L/K}(L^*)$. ■

3.4 Hilbert Symbol

We will prove the following proposition

Proposition 3.4.1. Let K be a local field containing a primitive nth root of 1. Any element of K^* that is a norm from every cyclic extension of K of degree dividing n is an nth power.

Example 3. We introduce a special case that $K = \mathbb{Q}_p$ and $n = 2$. For $a, b \in \mathbb{Q}_p^*$, define

$$(a,b)_p = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ -1 & \text{otherwise} \end{cases}$$

Clearly, $(a,b)_p$ depends only a, b modulo squares, and so there is a pairing

$$a, b \mapsto (a,b)_p : \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \to \{\pm 1\}$$

Also, one can verify that this pairing is bi-multiplicative, symmetric and non-degenerate.

Let a be a non-square in $\mathbb{Q}_p^*$. Thus,

$$\begin{aligned} b \text{ is a norm from } \mathbb{Q}_p[\sqrt{a}] &\iff b = (z - \sqrt{a}x)(z + \sqrt{a}x) \text{ has a solution in } \mathbb{Q}_p \\ &\iff (a,b)_p = 1 \end{aligned}$$

(Note: at this case, any y satisfying the equation $ax^2 + by^2 = z^2$ cannot be zero.

Thus, if b is in $\mathrm{Nm}(\mathbb{Q}_p[\sqrt{a}])$ for any a, then b is in $(\mathbb{Q}_p^*)^2$.

Definition 3.4.2. Now we define the Hilbert symbol in the general case.

From the sequence

$$0 \to \mu_n \to (K^{\mathrm{al}})^* \xrightarrow{x \mapsto x^n} (K^{\mathrm{al}})^n \to 0$$

and the Hilbert 90 theorem, we can obtain that

$$H^1(G, \mu_n) \cong K^*/(K^*)^n, \quad H^2(G, \mu_n) \cong H^2(G, (K^{\mathrm{al}})^*)_n$$

where $\square_n$ represents the elements in $\square$ killed by n.

Now we consider the cup-product

$$H^1(G, \mathbb{Z}/n\mathbb{Z}) \times H^1(G, \mu_n) \to H^2(G, \mu_n)$$

where I assume that G acts on $\mathbb{Z}/n\mathbb{Z}$ trivially. Thus, the cup-product becomes

$$\mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \times K^*/(K^*)^n \to H^2(G, (K^{\mathrm{al}})^*)_n$$

For $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^*/(K^*)^n$, we write (χ, b) for the image of the pair.

Let χ be an element with order n, let L_χ be the subfield fixed by $\mathrm{Ker}(\chi)$. Thus, it represents an extension with Galois group $G/\mathrm{Ker}(\chi) \cong \mathbb{Z}/n\mathbb{Z}$, that is, it is a cyclic extension of K.

Let $b \in K^*$, the local Artin map tells us that there is an isomorphism

$$K^*/\mathrm{Nm}L_\chi^* \xrightarrow{\sim} H^2(\mathbb{Z}/n\mathbb{Z}, L_\chi^*)$$

$$b \mapsto \delta\chi \cup b$$

The inflation map, which is injective, sends $\delta\chi \cup b$ to (χ, b). Thus, if $(\chi, b) = 0$ then $(\chi, b)' = 0$, through the isomorphism this indeed means that $b \in \mathrm{Nm}L_\chi^*$.

Considering that there is an isomorphism

$$\mathrm{Inv}_K : H^2(G, (K^{\mathrm{al}})^*) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

then there is a pairing

$$\text{the set of } (\chi, b) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

We can verify that the left kernel of this pairing is zero.

Now we assume that K is a local field containing the nth root of 1. Thus, $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ as G-modules. Then we have a cup-product pairing

$$H^1(G, \mu_n) \times H^1(G, \mu_n) \to H^2(G, \mu_n \otimes \mu_n)$$

which is exactly

$$K^*/(K^*)^n \times K^*/(K^*)^n \to \mu_n$$

This pairing is called the Hilbert symbol.

Theorem 3.4.3. This pairing has the following properties

1. It is bi-multiplicative.
2. It is skew-symmetric, i.e., $(b, a) = (a, b)^{-1}$.
3. It is non-degenerate.
4. $(a, b) = 1$ if and only if b is a norm from $K[\sqrt[n]{a}]$.

3.5 The existence theorem

Theorem 3.5.1. A subgroup N of K^* is a norm group if there is a finite Abelian extension L/K such that $\mathrm{Nm}_{L/K}(L^*) = N$. Then, every norm open subgroup of finite index in K^* is a norm group.

Proof. Step 1. For all finite extensions L/K, the norm map $L^* \to K^*$ has closed image and compact kernel.

By 1.1.9, the image is open and closed. For the kernel, it is closed in $\mathcal{O}_L^*$, thus is compact.

Step 2. Let $D_K = \bigcap_{L/K \text{ finite}} \mathrm{Nm}_{L/K}(L^*)$. For any finite extension K'/K, $\mathrm{Nm}_{K'/K} D_{K'} = D_K$.

Let $a \in D_K$, and consider the sets

$$\mathrm{Nm}_{L/K'}(L^*) \cap \mathrm{Nm}_{K'/K}^{-1}(a)$$

for L/K' finite. These sets are compact and non-empty, and the intersection of any two of them contains the third one. Thus, the intersection of all of them is non-empty. That means, $\mathrm{Nm}_{K/K'}$ is surjective over D_K.

Step 3. The group D_K is divisible.

Let $n > 1$ be an integer. We want to show that $D_K^n = D_K$. Let $a \in D_K$. For each finite extension L of K containing a primitive nth root of 1, consider the set

$$E(L) = \{b \in K^* | b^n = a, \quad b \in \mathrm{Nm}_{L/K}(L^*)\}$$

From step 2 we know that $a = \mathrm{Nm}_{L/K} a'$ for some $a' \in D_L$. From the Hilbert symbol theorem we know that a' is indeed a nth power, said $a' = c^n$ for $c \in L^*$. Thus, $a = \mathrm{Nm}(c)^n$. As a result, $E(L)$ is non-empty. Moreover, it is easy to see that

$$E(L) \cap E(L') \supseteq E(L \cdot L')$$

Also, note that $E(L)$ is a finite set. Thus, the intersection of all $E(L)$ is non-empty.

Step 4. Every subgroup I of finite index containing $\mathcal{O}_K^*$ is a norm subgroup.

The group I is just like $\mathrm{ord}_K^{-1}(n\mathbb{Z})$. Let K_n be the unramified extension of K of degree n. Then $\mathrm{Nm}_{K_n/K}(K_n^*)$ is a subgroup of K^* containing U_K with image $n\mathbb{Z}$. Thus, it is exactly I.

Step 5. The original theorem.

Let $\mathcal{N}$ be the set of all norm groups in K^*, so that $D_K = \bigcap_{N \in \mathcal{N}} N$. Let I be a subgroup of K^* of finite index. Because D_K is divisible, $I \supseteq D_K$. Thus, $I \supseteq \bigcap_{N \in \mathcal{N}} (N \cap \mathcal{O}_K^*)$. Because these sets are compact, and any two of them contains the third one, $I \supseteq N \cap \mathcal{O}_K^*$ for a certain N.

Now the group $\mathcal{O}_K^* \cdot (N \cap I)$ is a subgroup of finite index in K^* containing $\mathcal{O}_K^*$, which is a norm group. Now $N \cap (U_K \cdot (N \cap I))$, is an intersection of two norm groups, and thus contains a norm group. We can check easily that I contains this intersection, then it contains a norm group. Then I is a norm group. ■

4 Brauer Groups

4.1 Simple algebras; semisimple modules

Definition 4.1.1. A k-algebra is a ring A containing k in its center and **finite dimensional** as a k-vector space. A k-subalgebra of a k-algebra is a subring containing k.

A homomorphism $\varphi : A \to B$ of k-algebras is a homomorphism of rings with the property that $\varphi(a) = a$ for all $a \in k$.

Now we write A for a k-algebra.

Definition 4.1.2. By an A-module, we mean a **finitely generated** left A-module V.

An A-module is simple if it is nonzero and contains contains no proper A-submodule except 0, and it is semi-simple if it is isomorphic to a direct sum of simple A-modules. It is in-decomposable if it can not be written as a direct sum of two non-zero A-modules.

Every semi-simple A-module V can be written as a direct sum

$$V \cong m_1 S_1 \oplus \cdots \oplus m_r S_r$$

with each S_i simple and no two isomorphic. An A-module is said to be isotypic if $r < 2$.

Proposition 4.1.3. Let V be a semi-simple A-module. A submodule of V is stable under all endomorphisms of V if and only if it is a sum of isotypic components of V.

Definition 4.1.4. A k-algebra A is said to be semi-simple if every A-module is semi-simple.

Proposition 4.1.5. Let A be a semi-simple k-algebra. The isotypic components of the A-module ${}_AA$ are the minimal two-sided ideas of A.

Definition 4.1.6. A k-algebra A is said to be simple if it contains no proper two-sided ideals other than 0.

A k-algebra A is said to be a division algebra if every nonzero element a of A has an inverse. Note that a division algebra is almost a field except the commutativity. It also have the similar properties with fields, like a division algebra has no nonzero proper ideals, left, right, or two-sided, and so is simple.

Much of linear algebra does not require that the field be commutative. For example, we can define the dimension for a finite generated module V over a division algebra D.

Example 4. For $(a, b) \in k^*$, let $H(a, b)$ be the k-algebra with basis $1, i, j, ij$ (as a k-vector space) and with the multiplication determined by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji$$

Then $H(a, b)$ is a k-algebra, called a quaternion algebra over k.

Definition 4.1.7. Let A be a k-subalgebra of a k-algebra B. The centralizer of A in B is

$$C_B(A) = \{b \in B | ba = ab \text{ for all } a \in A\}$$

Theorem 4.1.8 (Double centralizer theorem)**.** Let A be a k-algebra, and let V be a faithful semi-simple A-module. Then $C(C(A)) = A$ (centralizers taken in $\mathrm{End}_k(V)$).

Proof. Let $D = C_{\mathrm{End}_k(V)}(A)$, and $B = C_{\mathrm{End}_k(V)}(D)$. Clearly, every $a \in A$ commutes with D. Thus, $A \subseteq B$. The following lemma gives us that $A \supseteq B$. ■

Lemma 4.1.9. For any $v_1, \cdots, v_n \in V$ and $b \in B$, there exists an $a \in A$ such that

$$av_1 = bv_1, \quad av_2 = bv_2, \cdots, av_n = bv_n$$

Lemma 4.1.10 (Schur's lemma)**.** The endomorphism algebra of a simple A-module is a division algebra.

Proof. The linear map between S, which is a simple A-module, is either 0 or a bijection. ■

Theorem 4.1.11. Every simple k-algebra A is isomorphic to $M_n(D)$ for some n and some division k-algebra D.

Proof. Choose a simple A-module S. Since the kernel of $A \to \mathrm{End}_k(S)$ will be a two-sided ideal of A, the action of A on S is indeed faithfully.

Let D be the centralizer of A in the k-algebra $\mathrm{End}_k(S)$ of k-linear maps $S \to S$. We know that $A = C_{\mathrm{End}_k(S)}(D)$. That is, $D = \mathrm{End}_A(S)$. Thus, Schur's lemma tells us that D is a division algebra. Therefore, S is a free D-module. Thus, $A \cong \mathrm{End}_D(S) \cong M_n(D^{\mathrm{op}})$. ■

Corollary 4.1.12. Simple k-algebras are semi-simple.

Theorem 4.1.13. Let A be a semi-simple k-algebra. The following conditions on A are equivalent:

1. A is simple
2. the A-module ${}_AA$ is isotypic
3. any two simple A-modules are isomorphic.

Corollary 4.1.14. Let A be a simple A-modules. Any two minimal left ideals of A are isomorphic as left A-modules, and A is a direct sum of its minimal left ideals.

Corollary 4.1.15. Let A be a simple A, and let S be a simple A-module. Every A-module is isomorphic to a direct sum of copies of S. Any two A-modules having the same dimension over k are isomorphic.

4.2 Definition of the Brauer Group

Proposition 4.2.1. Let A, A' be k-algebras, with sub-algebras B and B'. Let $C(B)$ and $C(B')$ be the centralizers of B and B' in A and A' separately. Then the centralizer of $B \otimes_k B'$ in $A \otimes_k A'$ is $C(B) \otimes_k C(B')$.

Corollary 4.2.2. The centre of a simple k-algebra is a field.

Proof. We have

$$Z(M_n(D)) = Z(k \otimes_k Z(D)) \cong Z(k) \otimes_k Z(D) = Z(D)$$

Obviously, the centre of a division algebra is a field. ■

Definition 4.2.3. A k-algebra is said to be centre if its centre is k.

Definition 4.2.4. Let V be a k-vector space, possibly infinite dimensional. Let $(e_i)_{i\in I}$ be a basis for V. Any $v \in V$ can be written uniquely $v \sum a_i e_i$, and we write

$$J(v) = \{i \in I | a_i \neq 0\}$$

it is a finite subset of I, which is empty if and only if $v = 0$.

Let W be a subspace of V. A nonzero element $w \in W$ is called primordial if at least one $a_i = 1$ and $\#J(W) = \min\{J(w')|w' \in W\}$.

Proposition 4.2.5. (a) Let w be a nonzero element of W such that $J(w)$ is minimal, and let w' be a second nonzero element of W. Then $J(w') \subseteq J(w)$ if and only if $w' = cw$.

(b) The set of primordial elements of W spans it.

Proposition 4.2.6. The tensor product of two central simple k-algebras is again central simple.

Theorem 4.2.7 (Skolem,Noether)**.** Let $f, g : A \to B$ be homomorphism from a k-algebra to a k-algebra B. If A is simple and B is central simple, then there exists an invertible element $b \in B$ such that $f(a) = b \cdot g(a) \cdot b^{-1}$ for all $a \in A$.

Corollary 4.2.8. Let A be a central simple algebra over k, and let B_1 and B_2 be simple k-subalgebras of A. Any isomorphism $f : B_1 \to B_2$ is induced by an inner automorphism of A, i.e., there exists an invertible $a \in A$ such that $f(b) = aba^{-1}$ for all $b \in B_1$.

Definition 4.2.9. Let A and B be central simple algebras over k. We say that A and B are similar, $A \sim B$, if $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$. Define $\mathrm{Br}(k)$ to be the set of similarity classes of central simple algebras over k. It is an Abelian group.

Note that $A \mapsto A \otimes_k K$ builds a homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(K)$$

its kernel is denoted by $\mathrm{Br}(K/k)$. An element in $\mathrm{Br}(K/k)$ is said to have a splitting field K.

Proposition 4.2.10. Note that $A \cong M_n(D)$ for some central division algebra D. As a result, each similarity is represented by a central division algebra.

Example 5. If k is algebraically closed, then $\mathrm{Br}(k) = 0$.

Proposition 4.2.11. Let A be a central simple algebra over k, and let K be a field extension containing k. Then $A \otimes_k K$ is a central simple algebra over K.

Corollary 4.2.12. For a central simple algebra A over k, $[A : k]$ is a square.

Proposition 4.2.13. For any field k, $\mathrm{Br}(k) = \bigcup \mathrm{Br}(K/k)$, where K runs over the finite extensions of k contained in some fixed algebraic closure.

4.3 The Brauer group and cohomology

We will prove that there is an isomorphism

$$H^2(\mathrm{Gal}(L/K), L^*) \cong \mathrm{Br}(L/K)$$

for any Galois extension L/K.

Theorem 4.3.1 (Another version of double centralizer theorem)**.** Let B be a simple k-subalgebra of a central simple k-algebra A. Then the centralizer $C = C(B)$ of B in A is simple, and B is the centralizer of C. Moreover,

$$[B : k][C : k] = [A : k]$$

Corollary 4.3.2. If in the statement of the theorem, B has center k, then so does C. The canonical homomorphism

$$B \otimes_k C \to A$$

is an isomorphism.

Corollary 4.3.3. Let A be a central simple algebra over k, and let L be a subfield of A containing k. The following are equivalent:

1. L equals its centralizer in A.
2. $[A : k] = [L : k]^2$.
3. L is a maximal commutative k-subalgebra of A.

Corollary 4.3.4. The maximal subfields containing k of a central division k-algebra D are exactly those with degree $\sqrt{[D : k]}$ over k.

Corollary 4.3.5. Let A be a central simple algebra over k. A field L of finite degree over k spits A if and only if there exists an algebra B similar to A containing L and such that

$$[B : k] = [L : k]^2$$

In particular, every subfield L of A of degree $[A : k]^{1/2}$ over k splits A.

Corollary 4.3.6. Let D be a central division algebra of degree n^2 over k, and let L be a field of degree n over k. Then L splits D if and only if L can be embedded in D.

Proposition 4.3.7. Every central division algebra over k contains a maximal subfield separable over k.

Corollary 4.3.8. The Brauer group $\mathrm{Br}(k) = \bigcup \mathrm{Br}(L/k)$, where L/K runs over the finite extensions of k contained in a fixed separable closure of k.

Define $\mathcal{A}(L/K)$ to be the class if central simple algebras A containing L and of degree $[A : k] = [L : k]^2$.

Fix an $A \in \mathcal{A}(L/K)$. Recall that there exists an element $e_\sigma \in A$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1},\ \forall a \in L$$

Through $\sigma\tau a = \sigma(\tau a)$ we can conclude that

$$e_{\sigma\tau} a e_{\sigma\tau}^{-1} = e_\sigma e_\tau a e_\tau^{-1} e_\sigma^{-1}$$

Thus, $e_\sigma e_\tau = \varphi(\sigma,\tau) e_{\sigma\tau}$ for some $\varphi \in L^*$.

One can verify that this defines a 2-cocycle. Thus, we have a well-defined map

$$A \mapsto \gamma(A) : \mathcal{A}(L/K) \to H^2(\mathrm{Gal}(L/K), L^*)$$

Theorem 4.3.9. The map γ is surjective, and its fibres are the isomorphism classes.

Theorem 4.3.10. For every finite Galois extension L/K, there is an isomorphism of Abelian groups

$$H^2(\mathrm{Gal}(L/K), L^*) \to \mathrm{Br}(L/K)$$

Corollary 4.3.11. For every separable algebraic closure K^{al} of K, there is a canonical isomorphism $\mathrm{Br}(K) \to H^2(\mathrm{Gal}_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*)$.

4.4 The Brauer groups of special fields

Theorem 4.4.1. For finite fields K, $\mathrm{Br}(k) \cong H^2(\mathrm{Gal}_{K^{\mathrm{al}}/K}, (K^{\mathrm{al}})^*) = 0$.

Theorem 4.4.2. Finite division algebras are commutative.

Theorem 4.4.3. If K is a local field, every element of $\mathrm{Br}(K)$ is split by an unramified extension. Thus $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{un}}/K)$.

5 Global Class Field Theory: Statements of the Main Theorems

5.1 Ray Class Groups

Let K be a number field and I the group of all fractional ideals of K. For any $a \in K$, let a_v or $a_{\mathfrak{p}}$ be the image of a in K_v or $K_{\mathfrak{p}}$.

Lemma 5.1.1. For any finite set S of primes of K, let I^S be the subgroup of I which is generated by the prime ideals not in S. Let

$$K^S = \{a \in K^* | (a) \in I^S\} = \{a \in K^* | \mathrm{ord}_{\mathfrak{p}}(a) = 0 \text{ for all } \mathfrak{p} \in S\}$$

Let $i : K^* \to I$ be the map sending a to the fractional ideal $a\mathcal{O}_K^*$.

Then there is an exact sequence

$$0 \to \mathcal{O}_K^* \to K^S \xrightarrow{i} I^S \to C = I/i(K^*) \to 0$$

Proof. To show $I^S \to C$ is surjective, it suffices to show that for any equivalent class in C, it can be represented by an element in I^S. We can reduce this question to the integral ideal case. For

integral ideal $\mathfrak{a} \in I^S$, we may write $\mathfrak{a} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}}\mathfrak{b}$, where $\mathfrak{b} \in I^S$. Choose a $\pi_\mathfrak{p} \in \mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$, then there exists an element a such that

$$a \equiv \pi_\mathfrak{p}^{n_\mathfrak{p}} (\mathrm{mod}\ \mathfrak{p}^{n_\mathfrak{p}+1})$$

for all $\mathfrak{p} \in S$. Then $(a) = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}}\mathfrak{b}'$, where $\mathfrak{b}' \in I^S$. Now $a^{-1}\mathfrak{a} \in I^S$. Since $(a) \mapsto 0$, $a^{-1}\mathfrak{a}$ is sent to $\mathfrak{a}$. ■

Definition 5.1.2. A modulus for K is a function

$$m : \{\text{primes of } K\} \to \mathbb{Z}$$

such that

(1) $m(\mathfrak{p}) \geq 0$ for all prime $\mathfrak{p}$ and $m(\mathfrak{p}) = 0$ for all but finite prime ideals $\mathfrak{p}$.

(2) if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) = 0$ or 1.

(3) if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

Let $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})} = \mathfrak{m}_\infty\mathfrak{m}_0$ formally be the ideal corresponding to m, where $\mathfrak{m}_\infty$ is the product of real primes. Let $S(\mathfrak{m})$ be the set of all primes dividing $\mathfrak{m}$.

Definition 5.1.3. For a modulus m, define $K_{\mathfrak{m},1}$ to be the set of $a \in K^*$ such that

$$\begin{cases} \mathrm{ord}_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) & \text{all finite } \mathfrak{p} \text{ dividing } \mathfrak{m} \\ a_\mathfrak{p} > 0 & \text{all real } \mathfrak{p} \text{ dividing } \mathfrak{m} \end{cases}$$

Note that for every $a \in K_{\mathfrak{m},1}$ and prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}$, $\mathrm{ord}_\mathfrak{p}(a) = 0$. Hence there is a natural inclusion $K_{\mathfrak{m},1} \to I^{S(m)}$ sending a to (a). The quotient $C_\mathfrak{m} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$ is called the (ray) class group modulo $\mathfrak{m}$.

Lemma 5.1.4. Let S be a finite set of prime ideals of K. Then every element $\alpha \in K^S$ can be written as $\alpha = a/b$ with $a, b \in \mathcal{O}_K \cap K^S$.

Proposition 5.1.5. Every class in $C_\mathfrak{m}$ is represented by an integral ideal $\mathfrak{a}$, and two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same class if and only if there exist nonzero $a, b \in \mathcal{O}_K$ such that $a\mathfrak{a} = b\mathfrak{b}$ and

$$a \equiv b \equiv 1 (\mathrm{mod}\ \mathfrak{m}_0)$$

$$a \text{ and } b \text{ have the same sign for every real prime dividing } \mathfrak{m}$$

Proof. Suppose that the class is represented by $\mathfrak{a} \in I^{S(\mathfrak{m})}$, let $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in $I^{S(\mathfrak{m})}$. By Chinese remainder theorem there exists a nonzero ideal in $c \in \mathfrak{c} \cap K_{\mathfrak{m}_0,1}$, and the strong approximation theorem shows that c can be chosen to be > 0 at the real primes. Now $c\mathfrak{a}$ is integral and represents the same class with $\mathfrak{a}$. ■

Theorem 5.1.6. For every modulus $\mathfrak{m}$ there is an exact sequence

$$0 \to \mathcal{O}_K^*/\mathcal{O}_K^* \cap K_{\mathfrak{m},1} \to K^{S(\mathfrak{m})}/K_{\mathfrak{m},1} \to C_\mathfrak{m} \to C \to 0$$

and canonical isomorphisms

$$K^{S(\mathfrak{m})}/K_{\mathfrak{m},1} \cong \prod_{\mathfrak{p} \text{ real and } \mathfrak{p}|\mathfrak{m}} \{\pm\} \times \prod_{\mathfrak{p} \text{ finite and } \mathfrak{p}|\mathfrak{m}} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^* \cong \prod_{\mathfrak{p} \text{ real and } \mathfrak{p}|\mathfrak{m}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^*$$

Therefore $C_{\mathfrak{m}}$ is a finite group of order

$$h_{\mathfrak{m}} = h \cdot (\mathcal{O}_K^* : \mathcal{O}_K^* \cap K_{\mathfrak{m},1})^{-1} 2^{r_0} \mathbb{N}(\mathfrak{m}_0) \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{\mathbb{N}\mathfrak{p}}\right)$$

where r_0 is the number of real primes dividing $\mathfrak{m}$ and $h = |C|$ is the class number.

Proof. The exactness of the sequence follows from 5.1.1. The second statement follows from the Chinese remainder theorem. ■

5.2 L-series and the Density of Primes in Arithmetic Progressions

5.3 The Main Theorems in Terms of Ideals

Definition 5.3.1. Let L/K be a finite Abelian extension with the Galois group G. For every finite set S of primes of K containing all primes that ramify in L, we have a homomorphism

$$\Psi : I^S \to \mathrm{Gal}(L/K), \quad \prod \mathfrak{p}_i^{n_i} \mapsto \prod \mathrm{Frob}_{\mathfrak{p}_i}^{n_i}$$

called the global Artin map (or reciprocity map).

Proposition 5.3.2. Let L be an Abelian extension of K, and let K' be an intermediate field: $L \supseteq K' \supseteq K$. Then the following diagram commutes:

$$\begin{array}{ccc} I_{K'}^S & \xrightarrow{\Psi_{L/K'}} & \mathrm{Gal}(L/K') \\ {\scriptstyle \mathrm{Nm}}\downarrow & & \downarrow \\ I_K^S & \xrightarrow{\Psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Corollary 5.3.3. Let $K' = L$, then $\mathrm{Nm}(I_L^S) \subseteq \mathrm{Ker}(\Psi_{L/K})$. Thus the Artin map induces a homomorphism

$$\psi_{L/K} : I_K^S / \mathrm{Nm}(I_K'^S) \to \mathrm{Gal}(L/K)$$

if L/K is a finite Abelian extension.

Definition 5.3.4. Let S be a finite set of primes of K. We say a homomorphism $\Psi : I^S \to G$ admits a modulus if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \supseteq S$ such that $\Psi(i(K_{\mathfrak{m},1})) = 0$. Thus Ψ admits a modulus if and only if it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$ with $S(\mathfrak{m}) \supseteq S$.

Theorem 5.3.5 (Reciprocity Law)**.** Let L be a finite Abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\Psi : I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, and it defines an isomorphism

$$I_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})}) \to \mathrm{Gal}(L/K)$$

A modulus as in the statement of the theorem is called a defining modulus for L.

Definition 5.3.6. We call that a subgroup H of $I_K^{\mathfrak{m}} = I_K^{S(\mathfrak{m})}$ is a congruence subgroup modulo $\mathfrak{m}$ if

$$I_K^{\mathfrak{m}} \supseteq H \supseteq i(K_{\mathfrak{m},1})$$

Theorem 5.3.7 (Existence theorem)**.** For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite Abelian extension L/K unramified at the primes not dividing $\mathfrak{m}$ such that $H = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}})$.

Remark 5.3.8. *Given a finite Abelian extension L/K, then the reciprocity law tells us that the Artin map $\Psi : I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ such that*

$$S(\mathfrak{m}) = S, \quad i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})}) = \mathrm{Ker}(\Psi)$$

In other word, there is an isomorphism

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/H \to \mathrm{Gal}(L/K)$$

The existing theorem tells us that L is highly connected with $\mathfrak{m}$, thus, we often note this L, called the ray class field modulo $\mathfrak{m}$, as $L_{\mathfrak{m}}$. For any field $L \subseteq L_{\mathfrak{m}}$, set

$$\mathrm{Nm}(C_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{\mathfrak{m}})$$

The existing theorem infers that the map $L \mapsto \mathrm{Nm}(C_{L,\mathfrak{m}})$ induces a bijection from the set of Abelian extensions of K contained in $L_{\mathfrak{m}}$ and the set of subgroups of $C_{\mathfrak{m}}$.

Corollary 5.3.9. For every number field K, there is an isomorphism

$$\varprojlim C_{\mathfrak{m}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

Corollary 5.3.10. Let $H = i(K_{\mathfrak{m},1})$, then for any modulus $\mathfrak{m}$ there is a field $L_{\mathfrak{m}}$, called the ray class field modulo $\mathfrak{m}$, such that there is an isomorphism

$$C_{\mathfrak{m}} \to \mathrm{Gal}(L_{\mathfrak{m}}/K)$$

Moreover, for any field $K \subseteq L \subseteq L_{\mathfrak{m}}$, define $\mathrm{Nm}(C_{L,\mathfrak{m}}) = \mathrm{Nm}(I_L^{\mathfrak{m}}) \subseteq C_{\mathfrak{m}}$. Then the correspondence $L \mapsto \mathrm{Nm}(C_{L,\mathfrak{m}})$ is a bijection between the set of Abelian extensions of K contained in $L_{\mathfrak{m}}$ and the set of subgroups of $C_{\mathfrak{m}}$. And

$$L_1 \subseteq L_2 \iff \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \supseteq \mathrm{Nm}(C_{L_2,\mathfrak{m}})$$

$$\mathrm{Nm}(C_{L_1 \cdot L_2,\mathfrak{m}}) = \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cap \mathrm{Nm}(C_{L_2,\mathfrak{m}})$$

$$\mathrm{Nm}(C_{L_1 \cap L_2,\mathfrak{m}}) = \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cdot \mathrm{Nm}(C_{L_2,\mathfrak{m}})$$

Definition 5.3.11. Let L/K be an Abelian extension with Galois group G. By the reciprocity law there is a modulus $\mathfrak{m}$, with $S = S(\mathfrak{m})$= the set of primes of K ramifying in L, such that the Artin map

$$\Psi_{L/K} : I^S \to G$$

has the kernel $i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})$.

Recall that there is an exact sequence

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^* \hookrightarrow K^S/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \xrightarrow{\Psi_{L/K}} G$$

there must be a smallest integer $f(\mathfrak{p}) \leq m(\mathfrak{p})$ such that the map factors as

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^* \to (\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^* \to G$$

Thus the modulus $\mathfrak{f}(L/K) = \mathfrak{m}_\infty \prod \mathfrak{p}^{f(\mathfrak{p})}$ is then the smallest modulus such that $\Psi_{L/K}$ factors through $C_\mathfrak{f}$, it is called the conductor of L/K. The condutor is divisible exactly by the prime ramifying in L.

The subfields of the ray class field $L_\mathfrak{m}$ containing K are those with conductor $\mathfrak{f}|\mathfrak{m}$. Every Abelian extension of K is contained in $L_\mathfrak{m}$ for some $\mathfrak{m}$.

Theorem 5.3.12 (Norm Limitation Theorem)**.** Let L be a finite extension of K, and let L' be a maximal Abelian subextension. For every defining modulus $\mathfrak{m}$ for L'

$$i(K_{\mathfrak{m},1})\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) = i(K_{\mathfrak{m},1})\mathrm{Nm}_{L'/K}(I_{L'}^{S(\mathfrak{m})})$$

5.4 Ideles

Definition 5.4.1. Define the group of ideles to be

$$\mathbb{I} = \mathbb{I}_K = \{(a_v) \in \prod K_v^* | a_v \in \mathcal{O}_v^* \text{ for all but finitely many } v\}$$

where $\mathcal{O}_v$ = the ring of integers in K_v.

For every finite set S of primes that includes all infinite primes, let

$$\mathbb{I}_S = \prod_{v\in S} K_v^* \times \prod_{v\notin S} \mathcal{O}_v^*$$

with the product topology. It is locally compact since the first factor is locally compact and the second factor is compact (by Tychonoff theorem). Note that

$$\mathbb{I} = \bigcup \mathbb{I}_S$$

Now we endow $\mathbb{I}$ a new topology, which is generated by the basis of open sets

$$\left\{\prod_v V_v : V_v \text{ is open in } K_v^* \text{ and } V_v = \mathcal{O}_v^* \text{ for all but finitely many } v\right\}$$

This topology makes every $\mathbb{I}_S$ open and inherits the product topology. Moreover, it makes $\mathbb{I}$ to be a topological group. The following sets form a fundamental system of neighborhood of 1: for each finite set of primes $S \supseteq S_\infty$ and $\epsilon > 0$, define

$$U(S,\epsilon) = \{(a_v) : |a_v - 1|_v < \epsilon, \text{ for } v \in S, \ |a_v|_v = 1, \text{ for } v \notin S\}$$

There is a canonical surjective homomorphism

$$id : (a_v) \mapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_{\mathfrak{p}_v}(a_v)} : \mathbb{I}_K \to I_K$$

whose kernel is $\mathbb{I}_{S_\infty}$.

Proposition 5.4.2. There is a canonical injective homomorphism

$$a \mapsto (a, a, \cdots) : K^* \to \mathbb{I}_K$$

The image of this homomorphism is discrete.

Proof. It suffices to show that the restriction of the topology on the image makes the single point set $\{1\}$ open.

Let $U = U(S, \epsilon) \ni 1$ with $S_\infty \subseteq S$ and $\epsilon < 1$. For $(a, a, \cdots) \in U$ and $v \notin S$, $|a|_v = 1$. Hence $|a-1|_v \leq 1$ for $v \notin S$. Thus we have $\prod |a-1|_v \leq \epsilon^{|S|}$, this contradicts the product formula unless $a = 1$. ■

Definition 5.4.3. If we identify K^* with its image in $\mathbb{I}_K$, we may define the idele class group of K to be the quotient $\mathcal{C} = \mathbb{I}/K^*$.

Definition 5.4.4. There is a canonical surjective homomorphism

$$c : (a_v) \mapsto \prod |a_v|_v : \mathbb{I} \to \mathbb{R}_{>0}$$

The image is called the content of (a_v). Define $\mathbb{I}^1 = \mathrm{Ker}(c)$. Obviously $K^* \subseteq \mathbb{I}^1$. The quotient $\mathbb{I}/K^*$ can not be compact since c is surjective, but $\mathbb{I}^1/K^*$ is compact.

Definition 5.4.5. Let $\mathfrak{m}$ be a modulus. For $\mathfrak{p}|\mathfrak{m}$, set

$$W_{\mathfrak{m}}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0}, & \mathfrak{p} \text{ real} \\ 1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})}, & \mathfrak{p} \text{ finite} \end{cases}$$

which is obviously a neighborhood of 1 in $K_{\mathfrak{p}}^*$. Note that when $\mathfrak{p}$ is finite, $W_{\mathfrak{m}}(\mathfrak{p}) \subseteq \mathcal{O}_{\mathfrak{p}}^*$.

Define $\mathbb{I}_{\mathfrak{m}}$ to be the set of ideles $(a_{\mathfrak{p}})_{\mathfrak{p}}$ such that $a_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}$:

$$\mathbb{I}_{\mathfrak{m}} = \left(\prod_{\mathfrak{p} \nmid \mathfrak{m}} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \right) \cap \mathbb{I}$$

Define $W_{\mathfrak{m}}$ to be the set of ideles $(a_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{I}_{\mathfrak{m}}$ such that $a_{\mathfrak{p}}$ is a unit for for all finite $\mathfrak{p}$ not dividing $\mathfrak{m}$:

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p} Nmid \mathfrak{m},\ \mathfrak{p} \text{ infinite}} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\mathfrak{p} Nmid \mathfrak{m},\ \mathfrak{p} \text{ finite}} \mathcal{O}_{\mathfrak{p}}^*$$

Note that $K_{\mathfrak{m},1} = K^* \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) = K^* \cap \mathbb{I}_{\mathfrak{m}}$ (recall that K^* can be identified as the diagonal in $\mathbb{I}$).

Proposition 5.4.6. Let $\mathfrak{m}$ be a modulus of K.

(a) The map $id : \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ defines an isomorphism

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m}\cdot 1} \cdot W_{\mathfrak{m}} \xrightarrow{\sim} C_{\mathfrak{m}}$$

(b) The inclusion $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}$ defines an isomorphism

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{\sim} \mathbb{I}/K^*$$

Proof. (a) Obviously $K_{\mathfrak{m}\cdot 1}$ is contained in the kernel of $\mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})} \to C_{\mathfrak{m}}$. Thus there is a homomorphism

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}}$$

Recall that $\mathbb{I}_{S_\infty} \cap \mathbb{I}_\mathfrak{m} = W_\mathfrak{m}$ is the kernel of id, hence the homomorphism

$$\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \cdot W_\mathfrak{m} \xrightarrow{\sim} C_\mathfrak{m}$$

is an isomorphism.

(2) The kernel of $\mathbb{I}_\mathfrak{m} \to \mathbb{I}/K^*$ is $K^* \cap \mathbb{I}_\mathfrak{m} = K_{\mathfrak{m},1}$. The surjectivity follows from the weak approximation theorem. ■

Proposition 5.4.7. Let $S \supseteq S_\infty$ be a finite set of primes and G an Abelian group. If $\psi : I^S \to G$ admits a modulus with $S = S(\mathfrak{m})$, then there exists a unique homomorphism $\phi : \mathbb{I} \to G$ such that

(a) ϕ is continuous (G with the discrete topology).

(b) $\phi(K^*) = 1$.

(c) $\phi(a) = \psi(id(a))$, for all $a \in \mathbb{I}^S \triangleq \{a \in \mathbb{I} | a_v = 1 \text{ for all } v \in S\}$

Proof. There is a diagram

$$\begin{array}{ccccc} & & I^\mathfrak{m} & \longrightarrow & C_\mathfrak{m} \xrightarrow{\psi} G \\ & & & & \cong\uparrow \\ & & \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m} \\ & & \cong\downarrow & & \\ \mathbb{I} & \longrightarrow & \mathbb{I}/K^* & & \end{array}$$

Define ϕ to be the composite $\mathbb{I} \to G$. ■

Remark 5.4.8. *The canonical homomorphism $\pi_\mathfrak{m} : \mathbb{I} \to C_\mathfrak{m}$ is the unique homomorphism satisfying*

(a) $\pi_\mathfrak{m}(K^*) = 1$.

(b) $\pi_\mathfrak{m}(a) = id(a)$ for all $a \in \mathbb{I}^{S(\mathfrak{m})}$.

If $\mathfrak{m}|\mathfrak{m}'$, then $\pi_\mathfrak{m}$ is precisely the map composing $\pi_\mathfrak{m}$ and $C_{\mathfrak{m}'} \to C_\mathfrak{m}$. Therefore, there is a continuous homomorphism $\pi : \mathbb{I} \to \lim_{\leftarrow} C_\mathfrak{m}$. This map is actually surjective.

Definition 5.4.9. Let L be a finite extension of K, let v be a prime of K. Recall that

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

then we may define

$$\mathrm{Nm}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K \quad (a_w) \mapsto (b_v) = (\prod_{w|v} \mathrm{Nm}_{L_w/K_v} a_w)$$

Proposition 5.4.10. There is a commutative diagram:

$$\begin{array}{ccccc} L^* & \longrightarrow & \mathbb{I}_L & \longrightarrow & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^* & \longrightarrow & \mathbb{I}_K & \longrightarrow & I_K \end{array}$$

5.5 The Main Theorem in Terms of Ideles

Lemma 5.5.1. Let L be a finite Abelian extension of K, let v be a prime of K and w one extension. Denote by $D(w)$ the decomposition group, which is isomorphic to $\mathrm{Gal}(L_w/K_v)$. The local class field theory tells us there is a homomorphism

$$\phi_v : K_v^* \to D(w) \subseteq G$$

Moreover, we have that the subgroup $D(w)$ and ϕ_v are independent of the choice of w.

Proposition 5.5.2. There exists a unique continuous homomorphism $\phi_K :: \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the following property: for any $L \subseteq K^{\mathrm{ab}}$ finite over K and any prime w of L lying over a prime v of K, the diagram

$$\begin{array}{ccc} K_v^* & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{a\mapsto\phi_K(a)|_L} & \mathrm{Gal}(L/K) \end{array}$$

commutes.

Proof. We may define

$$\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K) \quad a \mapsto \prod_v \phi_v(a_v)$$

and ϕ_K is the inverse limit. ■

Theorem 5.5.3 (Reciprocity Law)**.** The homomorphism $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ has the following properties:

(a) $\phi_K(K^*) = 1$

(b) for every finite Abelian extension L of K, ϕ_K defines an isomorphism

$$\phi_{L/K} : \mathbb{I}_K/(K^* \cdot \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K)$$

(b)' ϕ_K defines an isomorphism

$$\phi_{L/K} : \mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L) \to \mathrm{Gal}(L/K)$$

Theorem 5.5.4 (Existence Theorem)**.** Fix an algebraic closure K^{al} of K; for every open subgroup $N \subseteq \mathcal{C}_K$ of finite index, there exists a unique Abelian extension L of K contained in K^{al} such that $\mathrm{Nm}_{L/K}\mathcal{C}_L = N$.

Definition 5.5.5. A subgroup of $\mathcal{C}_K$ is a norm group if it is of the form $\mathrm{Nm}(\mathcal{C}_L)$ for some finite Abelian extension L of K, L is called the class field of K belonging to N.

6 L-series and the Density of Primes

6.1 Dirichlet series and Euler products

Definition 6.1.1. A Dirichlet series is a series of the form

$$f(s)=\sum_{n\geq 1}\frac{a(n)}{n^s},\quad a(n)\in\mathbb{C}, s=\sigma+it\in\mathbb{C}$$

An Euler product belonging to a number field K is a product of the form

$$g(s)=\prod_{\mathfrak{p}}\frac{1}{(1-\theta_1(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})\cdots(1-\theta_d(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})},\quad \theta_i(\mathfrak{p})\in\mathbb{C},\quad s\in\mathbb{C}$$

in which $\mathfrak{p}$ runs over all but finitely many of the prime ideals of $\mathcal{O}_K$.

6.2 Convergence Results

Proposition 6.2.1. Let

$$f(s)=\sum_{n\geq 1}\frac{a(n)}{n^s}$$

Write $S(x)=\sum_{n\leq x}a(n)$, and suppose that there exists positive constants a and b such that $|S(x)|\leq ax^b$ for all large x. Then the series $f(s)$ converges uniformly for s in

$$D(b,\delta,\epsilon)=\{\Re(s)\geq b+\delta,\quad |\arg(s-b)\leq\frac{\pi}{2}-\epsilon\}$$

for all $\delta,\epsilon>0$, and it converges to an analytic function on the half plane $\Re(s)>b$.

Lemma 6.2.2. The zeta function $\zeta(s)$ has an analytic continuation to a meromorphism function on $\Re(s)>0$ with its only (possible) pole at $s=1$.

Lemma 6.2.3. For s real and $s>1$,

$$\frac{1}{s-1}\leq\zeta(s)\leq 1+\frac{1}{s-1}$$

Hence $\zeta(s)$ has a simple pole at $s=1$ with residue 1, i.e.,

$$\zeta(s)=\frac{1}{s-1}+\text{holomorphic function near 1}$$

Proposition 6.2.4. Let $f(s)$ be a Dirichlet series for which there exist real constants C and b, $b<1$, such that

$$|S(n)-a_0n|\leq cn^b$$

Then $f(s)$ extends to a meromorphic function on $\Re(s)>b$ with a simple pole at $s=1$ with residue a_0, i.e., near $s=1$

$$f(s)=\frac{a_0}{s-1}+\text{holomorphic function}$$

near $s=1$.

Proposition 6.2.5. Let χ be a Dirichlet character of a number field K. For all s with $\Re(s) > 1$, the Euler product $\prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}}$ converges to $L(s,\chi)$.

Definition 6.2.6. Let K be a number field, let $\mathfrak{m}$ be a modulus. For every class $\mathfrak{l}$ in $C_\mathfrak{m} = I^\mathfrak{m}/i(K_{\mathfrak{m},1})$, we define the partial zeta function

$$\zeta(s,\zeta) = \sum_{\mathfrak{a}\geq 0, \mathfrak{a}\in\mathfrak{l}} \frac{1}{\mathbb{N}\mathfrak{a}^s}$$

Note that

$$L(s,\chi) = \sum_{\mathfrak{l}\in C_\mathfrak{m}} \chi(\mathfrak{l})\zeta(s,\mathfrak{l})$$

$$\zeta_K(s) = \sum_{\mathfrak{l}\in C_\mathfrak{m}} \zeta(s,\mathfrak{l})$$

Let $S(x,\mathfrak{l}) = |\{\mathfrak{a}\in\mathfrak{l} | \mathfrak{a} \text{ integral } \mathbb{N}\mathfrak{a}\leq x\}|$.

Theorem 6.2.7. The partial zeta function is analytic for $\Re(s) > 1 - \frac{1}{d}$ except a simple hole at $s = 1$.

6.3 Density of the Prime Ideals Splitting in an Extension

Definition 6.3.1. For a set of prime ideals of K, we define $\zeta_{K,T}(s) = \prod_{\mathfrak{p}\in T} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}$. If some positive integral power $\zeta_{K,T}(s)^n$ of $\zeta_{K,T}(s)$ extends to a meromorphic function on a neighborhood of 1 having a pole of order m at 1, then we say that T has polar density $\delta(T) = \frac{m}{n}$.

Proposition 6.3.2. (a) The set of all prime ideals of K has polar density 1.

(b) The polar density of every set (having one) is ≥ 0.

(c) Suppose that T is the disjoint union of T_1 and T_2. If any two of T, T_1, T_2 have polar densities, then so also does the third, and $\delta(T) = \delta(T_1) + \delta(T_2)$.

(d) If $T\subseteq T'$, then $\delta(T)\leq\delta(T')$ (when both are defined).

(e) A finite set has density 0.

Proposition 6.3.3. If T contains no primes for which $\mathbb{N}\mathfrak{p}$ is a prime, then $\delta(T) = 0$.

Corollary 6.3.4. Let T_1 and T_2 be sets of prime ideals in K. If the sets differ only by primes for which $\mathbb{N}\mathfrak{p}$ is not prime, also we assume that one of them has a polar density, then the other one has the same polar density.

Theorem 6.3.5. Let L be a finite extension of K, and let M be its Galois closure. Then the set of prime ideals of K that splits completely in L has density $\frac{1}{|M:K|}$.

6.4 Density of the Prime Ideals in an Arithmetic Progression

We omit some basic knowledge of Dirichlet density.

The key result is

Theorem 6.4.1. Let $\mathfrak{m}$ be a modulus for K, and let H be a congruence subgroup for $\mathfrak{m}$:

$$I^{\mathfrak{m}} \supseteq H \supseteq i(K_{\mathfrak{m},1})$$

Then

$$\delta(\{\mathfrak{p} \in H\}) = \begin{cases} \dfrac{1}{(I^{S(\mathfrak{m})} : H)}, & \text{if } L(1,\chi) \text{ is nonzero for all characters } \chi \neq \chi_0 \text{ of } I^{S(\mathfrak{m})}/H; \\ 0, & \text{otherwise} \end{cases}$$

Theorem 6.4.2. For every Galois extension L/K and modulus $\mathfrak{m}$ of K,

$$(I^{S(\mathfrak{m}):i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})})$$

7 Global Class Field Theory: Proofs of the Main Theorems

7.1 Outline

Note that we have constructed a homomorphism

$$\phi_{L/K} : \mathcal{C}_K \to \mathrm{Gal}(L/K)$$

We will verify the properties. We will first express the cohomology groups

$$H^0(G, \mathbb{I}_L) = \mathbb{I}_K$$

$$H^r(G, \mathbb{I}_L) = \bigoplus_v H_T^r(G^v, (L^V)^*)$$

Then, we will prove the following propositions

$$\text{for any cyclic extension } L/K,\ (\mathcal{C}_K : \mathrm{Nm}_{L/K}\mathcal{C}_L) \geq [L:K]$$

Also, we will prove the second inequality

Theorem 7.1.1. For every Galois extension L/K of number fields,

1. $(\mathcal{C}_K : \mathrm{Nm}_{L/K}\mathcal{C}_L) \leq [L:K]$;
2. $H^1(G, \mathcal{C}_L) = 1$;
3. $H^2(G, \mathcal{C}_L)$ has order $\leq [L:K]$.

7.2 The Cohomology of Ideles

Lemma 7.2.1. Let L/K be a finite Galois extension of number fields with Galois group G. Let v be a prime of K, then G acts on the set of the primes w of L which satisfy $w|v$.

Given a $w_0|v$. Let G_{w_0} be its decomposition group. For $\alpha \in \prod_{w|v} L_w$ and $\sigma \in G$, define $f_\alpha(\sigma) = \sigma(\alpha(\sigma^{-1}w_0))$. Then $f_\alpha \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$, and the map

$$\alpha \mapsto f_\alpha : \prod_{w|v} L_w \to \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$$

is an isomorphism of G-modules. Similar statements hold with L_w replaced with L_w^* and with $\mathcal{O}_{L_w}^*$.

Corollary 7.2.2. By Shapiro lemma, for all r,

$$H^r(G, \prod_{w|v} L_w^*) \cong H^r(G_{w_0}, L_{w_0}^*)$$

Remark 7.2.3. *The group $H^r(G_{w_0}, L_{w_0}^*)$ is independent of the choice of w_0 up to a canonical isomorphism. From now on we may set*

$$G^v = G_w, \quad L^v = L_w, \quad U^v = \mathcal{O}_{L_w}^*$$

Proposition 7.2.4. For all $r \geq 0$,

$$H_T^r(G, \mathbb{I}_L) \cong \bigoplus_v H_T^r(G^v, L^{v*})$$

Proof. Let $\mathbb{I}_{L,S} = \prod_{v\in S}(\prod_{w|v} L_w^*) \times \prod_{v\notin S}(\prod_{w|v} \mathcal{O}_{L_w}^*)$. Thus $\mathbb{I}_L$ is the direct union of all $\mathbb{I}_{L,S}$ and then

$$H^r(G, \mathbb{I}_L) = \varinjlim H^r(G, \mathbb{I}_{L,S}) = \varinjlim \left(\prod_{v\in S} H^r(G, \prod_{w|v} L_w^*) \times \prod_{v\notin S} H^r(G, \prod_{w|v} \mathcal{O}_{L_w}^*) \right)$$

The right hand is equal to $\prod_v H^r(G^v, L^{v*})$ by the corollary above. ■

Corollary 7.2.5. (a) $H^1(G, \mathbb{I}_L) = 0$.

(b) $H^2(G, \mathbb{I}_L) \cong \bigoplus_v (\frac{1}{n_v}\mathbb{Z}/\mathbb{Z})$, where $n_v = [L^v : K_v]$.

Lemma 7.2.6. If L/K is a finite cyclic extension of local fields, then $h(\mathcal{O}_L^*) = 1$ and $h(L^*) = [L : K]$.

Proof. From the exact sequence

$$0 \to \mathcal{O}_L^* \to L^* \to \mathbb{Z} \to 0$$

we can know that $h(L^*) = h(\mathbb{Z}) \cdot h(\mathcal{O}_L^*)$.

From the general local Artin map, we know that

$$|H^0(G_{L/K}, L^*)| = |G_{L/K}^{\mathrm{ab}}| = [L : K]$$

and

$$|H^1(G_{L/K}, L^*)| = |H_T^{-1}(G_{L/K}, \mathbb{Z})| = 1$$

■

Proposition 7.2.7. Let S be a finite set of primes of K, and let T be the set of primes of L lying over primes in S. If L/K is cyclic, then the Herbrand quotient

$$h(\mathbb{I}_{L,T}) = \prod_{v\in S} n_v$$

Proof. Recall that

$$\mathbb{I}_{L,T} = \left(\prod_{v\in S}(\prod_{w|v} L_w^*)\right) \times \left(\prod_{v\notin S}(\prod_{w|v} \mathcal{O}_{L_w}^*)\right)$$

By the lemma above, the herbrand quotient of $\mathbb{I}_{L,T}$ is equal to

$$\prod_{v\in S} h(G^v, L^{v*}) = \prod_{v\in S} n_v$$

■

Proposition 7.2.8. For every finite Galois extension L/K of number fields, $\mathrm{Nm}_{L/K}\mathbb{I}_L$ contains an open subgroup of $\mathbb{I}_K$ and therefore is itself open.

Proof. Let $S \supseteq S_\infty$ be the set of primes in K that ramify, and T the set of primes lying over S. Consider the subgroup $\mathrm{Nm}_{L/K}\mathbb{I}_{L,T} \subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L \subseteq \mathbb{I}_K$. By the theory of local fields,

$$\mathrm{Nm}_{L/K}\mathbb{I}_{L,T} = \prod_{v\notin S} \mathcal{O}_{K_v}^* \times \prod_{v\in S} (\text{an open subset of finite index in } K_v^*)$$

Thus $\mathrm{Nm}_{L/K}\mathbb{I}_{L,T}$ is open in $\mathbb{I}_{K,S}$ and then open in $\mathbb{I}_K$. ■

Remark 7.2.9. *The norm map $\mathrm{Nm}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ induces a norm map between $\mathcal{C}_L$ and $\mathcal{C}_K$, and there is a commutative diagram:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^* & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathcal{C}_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \\ 0 & \longrightarrow & K^* & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathcal{C}_K & \longrightarrow & 0 \end{array}$$

with every row exact. And further, there is an isomorphism

$$\mathbb{I}_K/K^* \cdot \mathrm{Nm}(\mathbb{I}_L) \to \mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L)$$

7.3 The Cohomology of the Units

Let L/K be a finite extension of number fields with Galois group G. Let $S \supseteq S_\infty$ be a finite set of primes of K, and let T be the set of primes of L lying over a prime of K in S. Define the group of T-units to be

$$U(T) = \{\alpha \in L | \mathrm{ord}_w(\alpha) = 0,\ \forall w \notin T\}$$

This is stable under G since T is.

We omit the proof of the following property.

Proposition 7.3.1. Assume that G is cyclic. Then

$$h(U(T)) = \frac{n}{\prod_{v\in S} n_v}$$

where $n = [L : K]$ and $n_v = [L^v : K_v]$.

7.4 Cohomology of the Idele Classes I: The first Inequality

Lemma 7.4.1. Let K be a number field, and let $S \supseteq S_\infty$ be a finite set of primes of K containing a set of generators for the ideal class group of K. Then

$$\mathbb{I}_K = K^* \cdot \mathbb{I}_S$$

Proof. The condition that S contains a set of generators for the ideal class group of K means that every fractional ideal $\mathfrak{a}$ can be written as

$$\mathfrak{a} = \mathfrak{b} \cdot (c)$$

where $\mathfrak{b} \in \langle S \rangle$ and (c) is a primary ideal. Therefore, every element in $I/\langle S \rangle$ can be represented by a primary fractional ideal. Thus, $I/\langle S \rangle \cdot i(K^*) = 0$.

Recall the map $\mathbb{I}_K \to I^S = I/\langle S \rangle$ defined by $(a_v) \to \prod_{v \in S} \mathfrak{p}_v^{\mathrm{ord}_{p_v}(a_v)}$ induces an isomorphism

$$\mathbb{I}/\mathbb{I}_S \to I^S$$

Thus,

$$\mathbb{I}/K^* \cdot \mathbb{I}_S \cong 0$$

■

Theorem 7.4.2. For any finite cyclic extension L/K of number fields, $h(\mathcal{C}_L) = [L : K]$.

Proof. Let $S \supseteq S_\infty$ be a finite set of primes such that S contains all primes that ramify in L and all primes below the set of $\mathfrak{P}$ which generates the ideal class group of L.

The last requirement actually means that $\mathbb{I}_L = \mathbb{I}_{L,T} \cdot L^*$, where T is a set of primes lying over a prime in S.

Then

$$\mathcal{C}_L = \mathbb{I}_L/L^* \cong \mathbb{I}_{L,T}/L^* \cap \mathbb{I}_T$$

Note that

$$L^* \cap \mathbb{I}_T = U(T)$$

we have $h(\mathcal{C}_L) = h(\mathbb{I}_{L,T})/h(U(T)) = [L : K]$. ■

Corollary 7.4.3 (The first inequality)**.** If L/K is a cyclic extension of degree n, then

$$(\mathbb{I}_K : K^* \cdot \mathrm{Nm}(\mathbb{I}_L)) \geq n$$

7.5 Cohomology of the Idele Classes II: The Second Inequality

Theorem 7.5.1. For every Galois extension L/K of number fields,

1. $(\mathcal{C}_K : \mathrm{Nm}_{L/K}\mathcal{C}_L) \leq [L : K]$;
2. $H^1(G, \mathcal{C}_L) = 1$;

3. $H^2(G, \mathcal{C}_L)$ has order $\leq [L : K]$.

Proof. Step 1. It suffices to show this theorem in the case that G is a p-group.

This follows from that the maps

$$\mathrm{Res} : H_T^r(G, M) \to H_T^r(H, M)$$

are surjective for all sylow p-subgroups H.

Step 2. It suffices to show this theorem in the case that G is a cyclic group of prime order p.

We can prove this step by induction on $[G : 1]$.

Step 3. When G is cyclic, all three statements are equivalent.

This is obvious.

For the rightness of (a) when G is cyclic, see 6.4.2. ■

7.6 Completion of the Proof of the Reciprocity Law

Theorem 7.6.1. (a) Let L/K be a finite Abelian extension of number fields. Then $\phi_{L/K}$ takes the value 1 on the principal ideles $K^* \subseteq \mathbb{I}_K$.

(b) Let L/K be a finite Galois extension of number fields. Then $\sum \mathrm{Inv}_v(\alpha) = 0$ for all $\alpha \in H^2(G_{L/K}, L^*)$.

Proof. Need to be created. ■

7.7 The Existence Theorem

Need to be created.