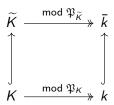
Local Class Field Theory

Yu-Hsuan Huang Che-Jui Chang Guan-Ting Chen

January 2020

Settings

Here, we refer to a local field as a non-Archimedean one. Suppose K be a local field with valuation v_K normalized such that $v_K(K^*)=\mathbb{Z}$. We denote the only maximal ideal \mathfrak{P}_K in K with uniformizer π_K . Finally we denote \mathcal{O}_K as the valuation ring and $U_K^{(n)}:=1+\mathfrak{P}_K^n, U_K:=U_K^{(0)}$. We denote \widetilde{K} the maximal unramified extension of K, k the residue field of \widetilde{K} and k be the algebraic closure of k. Note that k is also the residue field of \widetilde{K} . Thus we have the following inclusion diagram.



Since any finite sub-extension of \widetilde{K} share the same uniformizer with K and $\pi_K \in K$ is fixed by $\operatorname{Gal}(\widetilde{K}/K)$, we only need to specify how automorphism acts on residue field and thus.

$$\operatorname{\mathsf{Gal}}(\widetilde{K}/K) \cong \operatorname{\mathsf{Gal}}(\bar{k}/k)$$

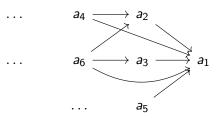
The residue field k is finite, thus easier to study.

Definition (Procyclic Group)

Let's first see a useful structure, the procyclic group,

$$\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} := \left\{ (a_n \mod n)_{1 \leq n} : \forall m \big| n, a_n = a_m \mod n \right\}.$$

An element in such projective limit could be thought as the following diagram where each arrow respect modular equivalence.



Theorem

Suppose $k \cong \mathbb{F}_q$. We have a natural isomorphism,

$$\operatorname{\mathsf{Gal}}(\bar{k}/k) \cong \lim_{\stackrel{\longleftarrow}{n}} \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

For $g \mapsto (a_n)_{n>1}$, we have

$$g\Big|_{\mathbb{F}_{q^n}}: x \mapsto x^{q^{a_n}}, \text{ for all } n.$$



Proof.

First of all, the map is clearly multiplicative. Then, by assumption, $\bar{k}\cong \bar{\mathbb{F}}_q=\bigcup_{n\geq 1}\mathbb{F}_{q^n}$. For $g\in \mathrm{Gal}(\bar{k}/k)$ restricting on finite subextension, we have,

$$\mathbf{g}\Big|_{\mathbb{F}_{q^n}} \in \langle \phi_q \rangle,$$

where $\phi_q: x \mapsto x^q$. Therefore, the map is surjective. On the other hand, if $g\Big|_{\mathbb{F}_{q^n}} = \mathrm{id}$, then $x^{q^{a_n}} = x, \forall x \in \mathbb{F}_{q^n} \subseteq \bar{k}$. Therefore $a_n = 1$ mod n and we have trivial kernel.

We could also regard $\widehat{\mathbb{Z}}$ as product of *p*-adic integers. Namely,

$$\lim_{\stackrel{\longleftarrow}{n}} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} \stackrel{\sim}{\longrightarrow} \prod_{p \text{ primes}} \mathbb{Z}_p,$$
$$(a_n)_{n \ge 1} \longmapsto (a_p)_{p \text{ primes}}.$$

This is trivially injective, and indeed surjective due to Chinese remainder theorem. For any $n \in \mathbb{Z}_{>0}$, write $n = \prod_{p \text{ primes}} p^{e_p}$ the prime factorization with $\forall' p : e_p = 0$, then we have,

$$\widehat{Z}/n\widehat{\mathbb{Z}}\cong \prod_{p \text{ primes}} \mathbb{Z}_p/n\mathbb{Z}_p\cong \prod_{p \text{ primes}} \mathbb{Z}_p/p^{e_p}\mathbb{Z}_p\cong \mathbb{Z}/n\mathbb{Z}.$$

Equip $\widehat{\mathbb{Z}}$ with the product topology from all \mathbb{Z}_p topology, those open groups within are exactly $n\widehat{\mathbb{Z}}$ where $n\in\mathbb{Z}$. On the other hand, given any (possibly infinite) Galois extension, Ω/K , we could also equip $\operatorname{Gal}(\Omega/K)$ with Krull topology, which is generated by the open sets $\sigma\operatorname{Gal}(\Omega/L)$, where $\sigma\in\operatorname{Gal}(\Omega/K)$ and L/K is any finite subextension.

Theorem (Infinite Galois Theory)

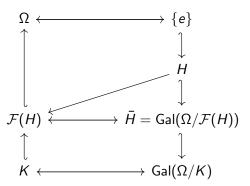
There is an bijective correspondence,

$$\{M/K: subextension \ of \ \Omega/K\} \longleftrightarrow \{H \leq \mathsf{Gal}(\Omega/K): H \ \textit{is closed}\}\,,$$

given by $M/K \mapsto \text{Gal}(\Omega/M)$ and $\{x \in \Omega : x \text{ fixed by } H\} \leftarrow H$.



Denote $\mathcal{F}(H)$ the fixed field of H, then $\operatorname{Gal}(\Omega/\mathcal{F}(H)) = \bar{H}$ is the topological closure of H, represented in the following diagram.



Proposition

Consider, $\sigma \in \operatorname{Gal}(\Omega/K)$, and Σ the fixed field of $\langle \sigma \rangle$, then $\operatorname{Gal}(\Omega/\Sigma)$ is a quotient of the procyclic group, $\widehat{\mathbb{Z}}$.

Proof.

Denote $G = \text{Gal}(\Omega/\Sigma)$, for every $n \in \mathbb{Z}_{>0}$ we have a surjective homomorphism,

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow G/G^n,$$

$$1 \mod n \longmapsto \sigma \mod G^n.$$

Running through n we get a continuous surjective homomorphism,

$$\widehat{\mathbb{Z}} \cong \lim_{\stackrel{\longleftarrow}{n}} \mathbb{Z}/n\mathbb{Z} \longrightarrow \lim_{\stackrel{\longleftarrow}{n}} G/G^n \cong G.$$



Definition

Suppose A is a multiplicative G module, and we denote $a^g := *(g, a), \forall g \in G, a \in A$. Then, define the following objects,

$$N_G : A \to N_G A, \quad a \mapsto \prod_{g \in G} a^g,$$
 $A_G := \{ a \in A : a^g = a, \forall g \in G \}, \quad I_G A := \{ a^{g-1} : a \in A, g \in G \}$ $H^0(G,A) := A_G/N_G A, \quad H^{-1}(G,A) := \ker N_G/I_G A.$

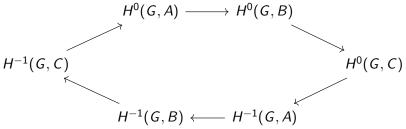
If $G = \langle \sigma \rangle$ is cyclic, then

$$I_GA = \left\{a^{\sigma^m-1} : m \in \mathbb{Z}\right\} = \left\{a^{(\sigma-1)(\sum_{0 \leq i < m} \sigma^i)} : m \in \mathbb{Z}\right\} = A^{\sigma-1}.$$

Suppose there is a exact sequence of G module,

$$1 \to A \to B \to C \to 1.$$

Then there is a exact hexagon.



We define the Herbrand quotient as fraction of diagonal sizes, $h(G,A) := \frac{\#H^0(G,A)}{\#H^{-1}(G,A)}$ when both are finite.

With cyclic condition, if A is finite, the exact sequences

$$1 \to A_G \to A \overset{\sigma-1}{\to} I_G A \to 1, \quad 1 \to \ker N_G \to A \overset{N_G}{\to} N_G A \to 1,$$

would yield $\#A = \#A_G \cdot \#I_GA = \# \ker N_G \cdot \#N_GA$ thus h(G,A) = 1.

Proposition

Suppose A is possibly infinite but G is finite and $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ is exact, then we have,

$$h(G,B) = h(G,A) \cdot h(G,C).$$

Finally, we see some useful facts without proof.

Theorem

Suppose L/K cyclic extension of local fields. Then,

$$\#H^0(\operatorname{\mathsf{Gal}}(L/K),L^{ imes})=[L:K],\quad \#H^{-1}(\operatorname{\mathsf{Gal}}(L/K),L^{ imes})=1.$$

Theorem

Suppose L/K is a finite unramified extension, then

$$\#H^0(Gal(L/K), U_L^{(n)}) = \#H^{-1}(Gal(L/K), U_L^{(n)}) = 1,$$

for all $n \in \mathbb{Z}_{>0}$.

The map $d_{L/K}$

Our goal in this part is to construct a canonical homomorphism

$$r_{L/K}: G(L/K) \to K^{\times}/N_{L/K}L^{\times}.$$

To do so, the concept about "Frobenius automorphism" plays an important role. Let L/K be finite Galois, $\phi_K \in G(\widetilde{K}/K)$ be a Frobenius automorphism and let d_K be an isomorphism

$$d_K: G(\widetilde{K}/K) \stackrel{\sim}{\longrightarrow} \widehat{\mathbb{Z}}$$

such that $d_K(\phi_K) = 1 \in \widehat{\mathbb{Z}}$.

The map $d_{L/K}$

Our goal in this part is to construct a canonical homomorphism

$$r_{L/K}: G(L/K) \to K^{\times}/N_{L/K}L^{\times}.$$

To do so, the concept about "Frobenius automorphism" plays an important role. Let L/K be finite Galois, $\phi_K \in G(\widetilde{K}/K)$ be a Frobenius automorphism and let d_K be an isomorphism

$$d_K: G(\widetilde{K}/K) \stackrel{\sim}{\longrightarrow} \widehat{\mathbb{Z}}$$

such that $d_K(\phi_K)=1\in\widehat{\mathbb{Z}}.$ Then we could define another map

$$d_{L/K}: G(\widetilde{L}/K) \longrightarrow \widehat{\mathbb{Z}}$$

$$\sigma \longmapsto d_K(\sigma \mid_{\widetilde{K}})$$

The map $d_{L/K}$

Our goal in this part is to construct a canonical homomorphism

$$r_{L/K}: G(L/K) \to K^{\times}/N_{L/K}L^{\times}.$$

To do so, the concept about "Frobenius automorphism" plays an important role. Let L/K be finite Galois, $\phi_K \in G(\widetilde{K}/K)$ be a Frobenius automorphism and let d_K be an isomorphism

$$d_K: G(\widetilde{K}/K) \stackrel{\sim}{\longrightarrow} \widehat{\mathbb{Z}}$$

such that $d_K(\phi_K)=1\in\widehat{\mathbb{Z}}.$ Then we could define another map

$$d_{L/K}: G(\widetilde{L}/K) \longrightarrow \widehat{\mathbb{Z}}$$

$$\sigma \longmapsto d_K(\sigma \mid_{\widetilde{K}})$$

In particular, if $\phi_L \in G(\widetilde{L}/L)$ is a Frobenius automorphism, then $\phi_L \mid_{\widetilde{K}} = \phi_K^{f(L/K)}$. Thus

$$d_{L/K}(\phi_L) = d_K(\phi_K^{f(L/K)}) = f(L/K)$$



The set $Frob(\widetilde{L}/K)$

We define a subset of $G(\widetilde{L}/K)$:

$$\operatorname{\mathsf{Frob}}(\widetilde{L}/{\mathsf{K}}) := \{ \sigma \in \mathcal{G}(\widetilde{L}/{\mathsf{K}}) \mid d_{L/{\mathsf{K}}}(\sigma) \in \mathbb{N} \} = d_{L/{\mathsf{K}}}^{-1}(\mathbb{N}).$$

The set $Frob(\widetilde{L}/K)$

We define a subset of $G(\widetilde{L}/K)$:

$$\operatorname{\mathsf{Frob}}(\widetilde{L}/K) := \{ \sigma \in \mathcal{G}(\widetilde{L}/K) \mid d_{L/K}(\sigma) \in \mathbb{N} \} = d_{L/K}^{-1}(\mathbb{N}).$$

In other words, $\sigma \in \text{Frob}(\widetilde{L}/K)$ iff $\sigma \mid_{K} = \phi_{K}^{n}$ for some $n \in \mathbb{N}$.

The set $Frob(\widetilde{L}/K)$

We define a subset of $G(\widetilde{L}/K)$:

$$\operatorname{\mathsf{Frob}}(\widetilde{L}/{\mathsf{K}}) := \{ \sigma \in {\mathsf{G}}(\widetilde{L}/{\mathsf{K}}) \mid d_{L/{\mathsf{K}}}(\sigma) \in \mathbb{N} \} = d_{L/{\mathsf{K}}}^{-1}(\mathbb{N}).$$

In other words, $\sigma \in \operatorname{Frob}(\widetilde{L}/K)$ iff $\sigma \mid_K = \phi_K^n$ for some $n \in \mathbb{N}$.

Proposition

For a finite Galois extension L/K, the mapping

$$Frob(\widetilde{L}/K) \longrightarrow G(L/K)$$
 $\sigma \longmapsto \sigma \mid_{L}$

is surjective.

Thus every element $\sigma \in G(L/K)$ can be extended to an element in $Frob(\widetilde{L}/K)$.

The fixed field Σ of $\sigma \in \text{Frob}(\widetilde{L}/K)$

Proposition

Let $\sigma \in Frob(\widetilde{L}/K)$ and let $\Sigma = \{a \in \widetilde{L} \mid a^{\sigma} = a\}$ be the fixed field of σ . Then

- 1. $\widetilde{\Sigma} = \widetilde{L}$ (i.e. Their maximal unramified extension coincide.)
- 2. $f(\Sigma/K) = d_{L/K}(\sigma)$
- 3. $e(\Sigma/K) = e(L/K)$.

In particular, Σ/K is a finite extension since

$$[\Sigma : K] = f(\Sigma/K)e(\Sigma/K) = d_{L/K}(\sigma)e(L/K) < \infty.$$

The fixed field Σ of $\sigma \in \text{Frob}(L/K)$

Proposition

Let $\sigma \in Frob(\widetilde{L}/K)$ and let $\Sigma = \{a \in \widetilde{L} \mid a^{\sigma} = a\}$ be the fixed field of σ . Then

- 1. $\widetilde{\Sigma} = \widetilde{L}$ (i.e. Their maximal unramified extension coincide.)
- 2. $f(\Sigma/K) = d_{L/K}(\sigma)$
- 3. $e(\Sigma/K) = e(L/K)$.

In particular, Σ/K is a finite extension since

$$[\Sigma : K] = f(\Sigma/K)e(\Sigma/K) = d_{L/K}(\sigma)e(L/K) < \infty.$$

Definition

The reciprocity map is defined by

$$r_{\widetilde{L}/K}: \mathsf{Frob}(\widetilde{L}/K) \longrightarrow K^{ imes}/N_{L/K}(L^{ imes})$$
 $\sigma \longmapsto N_{\Sigma/K}(\pi_{\Sigma}) \mod N_{L/K}(L^{ imes}),$

where Σ is the fixed field of σ .



Properties about the reciprocity map $r_{\widetilde{L}/K}$

One can show that $r_{\widetilde{L}/K}$ is well-defined, that is, if π_{Σ} and π'_{Σ} are both uniformizers of Σ , then

$$N_{\Sigma/K}(\pi_{\Sigma}) \equiv N_{\Sigma/K}(\pi_{\Sigma}') \mod N_{L/K}(L^{\times}).$$

Properties about the reciprocity map $r_{\widetilde{L}/K}$

One can show that $r_{\widetilde{L}/K}$ is well-defined, that is, if π_{Σ} and π'_{Σ} are both uniformizers of Σ , then

$$N_{\Sigma/K}(\pi_{\Sigma}) \equiv N_{\Sigma/K}(\pi'_{\Sigma}) \mod N_{L/K}(L^{\times}).$$

Proposition

If L/K is finite Galois, then the reciprocity map $r_{\widetilde{L}/K}$ is multiplicative.

This proposition is not trivial: we need to prove that for i = 1, 2, 3, given $\sigma_i \in \operatorname{Frob}(\widetilde{L}/K)$ and Σ_i is the fixed field of σ_i , then

$$N_{\Sigma_1/K}(\pi_{\Sigma_1})N_{\Sigma_2/K}(\pi_{\Sigma_2}) \equiv N_{\Sigma_3/K}(\pi_{\Sigma_3}) \mod N_{L/K}(L^{\times}).$$



The reciprocity homomorphism

Proposition

for every finite Galois extension L/K, there is a canonical homomorphism

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

 $\sigma \longmapsto N_{\Sigma/K}(\pi_{\Sigma}) \mod N_{L/K}(L^{\times}),$

where Σ is the fixed field of an extension $\widetilde{\sigma} \in Frob(\widetilde{L}/K)$ of $\sigma \in G(L/K)$.

We claim that this map is well-defined. (It is a homomorphism since $r_{\widetilde{L}/K}$ is.)

The reciprocity homomorphism $r_{L/K}$ is well-defined

Proof.

Let $\widetilde{\sigma}, \widetilde{\sigma}' \in \operatorname{Frob}(\widetilde{L}/K)$ be two extensions of $\sigma \in G(L/K)$ and Σ, Σ' be their fixed fields, resp. If $d_{L/K}(\widetilde{\sigma}) = d_{L/K}(\widetilde{\sigma}')$, then $\widetilde{\sigma} = \widetilde{\sigma}'$ are identical in both L and \widetilde{K} . Thus they are also identical in their compositum \widetilde{L} , that is, $\widetilde{\sigma} = \widetilde{\sigma}'$.

The reciprocity homomorphism $r_{L/K}$ is well-defined

Proof.

Let $\widetilde{\sigma}, \widetilde{\sigma}' \in \operatorname{Frob}(\widetilde{L}/K)$ be two extensions of $\sigma \in G(L/K)$ and Σ, Σ' be their fixed fields, resp. If $d_{L/K}(\widetilde{\sigma}) = d_{L/K}(\widetilde{\sigma}')$, then $\widetilde{\sigma} = \widetilde{\sigma}'$ are identical in both L and \widetilde{K} . Thus they are also identical in their compositum \widetilde{L} , that is, $\widetilde{\sigma} = \widetilde{\sigma}'$. Therefore WLOG, we may assume

$$d_{L/K}(\widetilde{\sigma}) < d_{L/K}(\widetilde{\sigma}').$$

Let $\tau = \widetilde{\sigma}'\widetilde{\sigma}^{-1}$, then $d_{L/K}(\tau) = d_{L/K}(\widetilde{\sigma}') - d_{L/K}(\widetilde{\sigma}) \in \mathbb{N}$. So $\tau \in \operatorname{Frob}(\widetilde{L}/K)$. Let T be the fixed field of τ . Since $\tau(a) = a$ for all $a \in L$, we have $T \supseteq L$. In particular,

$$N_{T/K}(\pi_T) = N_{L/K}(N_{T/L}(\pi_T)) \in N_{L/K}(L^{\times}).$$

So

$$\textit{N}_{\Sigma'/K}(\pi_{\Sigma'}) \equiv \textit{N}_{T/K}(\pi_T) \textit{N}_{\Sigma/K}(\pi_{\Sigma}) \equiv \textit{N}_{\Sigma/K}(\pi_{\Sigma}) \mod \textit{N}_{L/K}(\textit{L}^{\times}).$$



Main theorem

Let G(L/K)' be the commutator subgroup of G(L/K), and let $G(L/K)^{ab} = G(L/K)/G(L/K)'$. Since $r_{L/K}(G(L/K)') = \{1\} \subset K^{\times}/N_{L/K}L^{\times}$, $r_{L/K}$ naturally induces the homomorphism

$$\hat{r}_{L/K}: G(L/K)^{ab} \to K^{\times}/N_{L/K}L^{\times}.$$

Theorem (Local Reciprocity Law)

For every finite Galois extension L/K of non-archimedean local field, $\hat{r}_{L/K}$ is an isomorphism.

Proposition

If L/K is a finite unramified extension, then $r_{L/K}$ is an isomorphism.

Proof.

Since
$$\widetilde{L}=\widetilde{K}$$
 and $\widetilde{K}^{\phi_K}=K$

$$\Rightarrow r_{L/K}(\phi_K \mid_L) \equiv \pi_K \mod N_{L/K} L^{\times}.$$

Note that v_K induces an surjective homomorphism

$$K^{\times}/N_{L/K}L^{\times} \to \mathbb{Z}/n\mathbb{Z}, n = [L:K].$$

Since L/K is a cyclic extension,

$$\Rightarrow \#K^{\times}/N_{L/K}L^{\times} = \#H^0(G(L/K), L^{\times}) = n,$$

$$\Rightarrow K^{\times}/N_{L/K}L^{\times} \simeq \mathbb{Z}/n\mathbb{Z}$$
, and so π_K generates $K^{\times}/N_{L/K}L^{\times}$.

Since
$$\phi_K \mid_L$$
 generates $G(L/K)$ and $\#G(L/K) = \#K^{\times}/N_{L/K}L^{\times}$,

 $\Rightarrow r_{L/K}$ is an isomorphism.

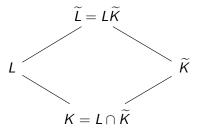


Proposition

If L/K is a finite totally ramified cyclic extension, then $r_{L/K}$ is an isomorphism.

Proof.

Since L/K is totally ramified, therefore $K = L \cap K$.



We have an isomorphism

$$G(\widetilde{L}/\widetilde{K}) \stackrel{\sim}{\to} G(L/K)$$
, by restriction $|_L$.

Let $\widetilde{\sigma}$ be a generator of $G(\widetilde{L}/\widetilde{K})$, $\sigma = \widetilde{\sigma} \mid_L$, and let $\sigma' = \widetilde{\sigma}\phi_L \in G(\widetilde{L}/K)$, $\Sigma = \widetilde{L}^{\sigma'}$, so $\sigma' \mid_L = \widetilde{\sigma} \mid_L = \sigma$.

We know $f_{\Sigma/K} = d_{L/K}(\sigma') = d_K(\sigma' \mid_K) = d_K(\phi_L \mid_{\widetilde{K}}) = f_{L/K} = 1.$

Let M/K be a finite galois subextension of \widetilde{L}/K containing Σ and L, and let $M_0=M\cap\widetilde{K}$.

 $\Rightarrow \widetilde{M} = \widetilde{L} = \widetilde{\Sigma}$, therefore we have

$$G(\widetilde{L}/\widetilde{K}) \stackrel{=}{\longrightarrow} G(\widetilde{M}/\widetilde{K}) \stackrel{=}{\longrightarrow} G(\widetilde{\Sigma}/\widetilde{K})$$

$$\simeq \Big|_{|L} \qquad \simeq \Big|_{|M} \qquad \simeq \Big|_{|\Sigma}$$

$$G(L/K) \stackrel{|L}{\longleftarrow} G(M/M_0) \stackrel{|\Sigma}{\longrightarrow} G(\Sigma/K)$$

Hence $N_{M/M_0}|_{\Sigma} = N_{\Sigma/K}$ and $N_{M/M_0}|_{L} = N_{L/K}$.



Claim : If
$$r_{L/K}(\sigma^m) \equiv 1 \mod N_{L/K}L^{\times}$$
 whit $0 \leq m < n = [L:K]$ then $m = 0$.

Assume this. Then $r_{L/K}$ is injective.

Since
$$\#K^{\times}/N_{L/K}L^{\times} = n = \#G(L/K)$$
, so $r_{L/K}$ is an isomorphism.

If now
$$r_{L/K}(\sigma^m) \equiv 1 \mod N_{L/K}L^{\times}$$
 with $0 \leq m < n$.

Let $\pi_L \in L$, $\pi_{\Sigma} \in \Sigma$ be prime elements,

$$\Rightarrow \pi_L$$
, π_{Σ} are both prime elements of M ,

$$\Rightarrow \pi_{\Sigma}^{m} = u \pi_{L}^{m} \text{ for some } u \in U_{M}$$
,

$$\begin{split} \Rightarrow 1 &\equiv \mathit{r}_{L/K}(\sigma^m) \equiv \mathit{N}_{\Sigma/K}(\pi^m_\Sigma) \\ &\equiv \mathit{N}_{M/M_0}(u) \mathit{N}_{L/K}(\pi^m_L) \equiv \mathit{N}_{M/M_0}(u) \;\; \mathsf{mod} \;\; \mathit{N}_{L/K}L^\times. \end{split}$$

$$\Rightarrow \exists \epsilon \in U_L \text{ such that } N_{L/K}(\epsilon) = N_{M/M_0}(u).$$

Since
$$G(M/M_0)$$
 is cyclic, so $\#H^{-1}(G(L/K), L^{\times}) = 1$,
 $\Rightarrow \exists a \in M^{\times}$ such that $u^{-1}\epsilon = a^{\widetilde{\sigma}-1}$,
 $\Rightarrow (\pi_L^m \epsilon)^{\widetilde{\sigma}-1} = (\pi_L^m \epsilon)^{\sigma'-1} = (\pi_{\Sigma}^m a^{\widetilde{\sigma}-1})^{\sigma'-1} = (a^{\sigma'-1})^{\widetilde{\sigma}-1}$,

$$\Rightarrow b := \pi_I^m \epsilon a^{\sigma'-1} \in M_0^{\times} \text{ with } v_M(b) = m.$$

Since
$$v_M(b) = e_{M/M_0} v_{M_0}(b) = n v_{M_0}(b)$$
,

$$\Rightarrow n \mid m$$
, therefore $m = 0$.

Proposition

Let L/K and L'/K' be finite galois extensions such that K'/K and L'/L are finite separable extensions. Then we have the commutative diagram

$$\begin{array}{ccc} G(L'/K') & \xrightarrow{|_L} & G(L/K) \\ & & \downarrow^{r_{L'/K'}} & & \downarrow^{r_{L/K}} \\ K'^{\times}/N_{L'/K'}L'^{\times} & \xrightarrow{N_{K'/K}} & K^{\times}/N_{L/K}L^{\times} \end{array}$$

Proof.

Given
$$\sigma' \in G(L'/K')$$
, let $\sigma = \sigma' \mid_{L} \in G(L/K)$.
If $\widetilde{\sigma'} \in Frob(\widetilde{L'}/K')$ such that $\widetilde{\sigma'} \mid_{L'} = \sigma'$,
 $\Rightarrow \widetilde{\sigma} := \widetilde{\sigma'} \mid_{\widetilde{L}} \in Frob(\widetilde{L}/K)$ (since $d_{L/K}(\widetilde{\sigma}) = f_{K'/K} d_{L'/K'}(\widetilde{\sigma'}) \in \mathbb{N}$)
and $\widetilde{\sigma} \mid_{L} = \sigma$.

Let
$$\Sigma' = \widetilde{L'}^{\widetilde{\sigma'}}$$
, and let $\Sigma = \widetilde{L}^{\widetilde{\sigma}} = \Sigma' \cap \widetilde{L} = \Sigma' \cap \widetilde{\Sigma}$, $\Rightarrow f_{\Sigma'/\Sigma} = 1$.

If now $\pi_{\Sigma'}$ is a prime element of Σ' then $\pi_{\Sigma} := N_{\Sigma'/\Sigma}(\pi_{\Sigma'})$ is a prime element of Σ ,

$$\Rightarrow N_{\Sigma/K}(\pi_{\Sigma}) = N_{\Sigma/K}(N_{\Sigma'/\Sigma}(\pi_{\Sigma'})) = N_{K'/K}(N_{\Sigma'/K'}(\pi_{\Sigma'})). \quad \Box$$

Corollary

Let M/K be a galois subextension of a finite galois extension L/K. Then we have the commutative exact diagram

Proof.

Since
$$K^{\times}/N_{M/K}M^{\times} \simeq \frac{K^{\times}/N_{L/K}L^{\times}}{N_{M/K}M^{\times}/N_{L/K}L^{\times}}$$
.



Proof of Local Reciprocity Law.

Case 1 : Suppose L/K is a cyclic extension.

Let
$$M = L \cap \widetilde{K}$$
,

 \Rightarrow L/M is a totally ramified cyclic extension, and M/K is a unramified extension.

Since L/K, L/M, M/K are cyclic extension, $\Rightarrow \#K^{\times}/N_{L/K}L^{\times} = (\#M^{\times}/N_{L/M}L^{\times})(\#K^{\times}/N_{M/K}M^{\times}).$

Thus, we have

Hence $\hat{r}_{L/K} = r_{L/K}$ is an isomorphism.

Case 2 : Suppose L/K is an abelian extension but not cyclic.

We prove this by induction on [L:K].

Note that
$$G(L/K) = \bigoplus_{i=1}^{\ell} H_i$$
 for some cyclic subgroups H_i , $\ell > 1$.

Let $M_i = L^{H_i}$. Then

$$\Rightarrow r_{L/K}$$
 is surjective, and $\ker(r_{L/K}) \subset \bigcap_{i=1}^{\ell} G(L/M_i) = \bigcap_{i=1}^{\ell} H_i = \{1\}$
 $\Rightarrow \hat{r}_{L/K} = r_{L/K}$ is an isomorphism.

Case 3 : Suppose L/K is not abelian extension.

We prove this by induction on [L:K].

Let H be the commutator subgroup of G(L/K), and let $M = L^H$. In fact, a finite galois extension of non-archimedean local fields is always a solvable extension. Hence $\{1\} \neq H \neq G(L/K)$.

We have

 $\Rightarrow r_{L/K}$ is surjective, and $\ker(r_{L/K}) = G(L/M) = H$,

 $\Rightarrow \hat{r}_{L/K}$ is an isomorphism.



Corollary

Let L/K be a finite galois extension of non-archimedean local field, and let L^{ab}/K be the maximal abelian subextension in L/K. Then $N_{L/K}L^{\times}=N_{L^{ab}/K}L^{ab^{\times}}$.

Proof.

Since
$$G(L/K)^{ab} = G(L^{ab}/K)$$
.



References



J. Neukirch, Algebraic Number Theory, Springer, 1999