A BRIEF INTRODUCTION ON LOCAL CLASS FIELD THEORY

HUA-CHIEH LI

In [4] Neukirch wrote: "The main goal of field theory is to classify all algebraic extensions of a given field K. The law governing the constitution of extensions of K is hidden in the inner structure of the base field K itself, and should therefore be expressed in terms of entities directly associated with it." Local class field theory solves this problem as far as the abelian extensions of the local field K are concerned. It establishes a one-to-one correspondence between these extensions and certain subgroups of K^*. More precisely, the rule

$$L \to N_{L/K}L^*$$

gives a one-to-one correspondence between the finite abelian extensions of a local field K and the open subgroups of finite index in K^*. This is called the *existence theorem*, because its essential statement is that, for every open subgroup $\mathcal{N}$ of finite index in K^*, there exists an abelian extension L/K such that $\mathcal{N} = N_{L/K}L^*$. This is the "class field" of $\mathcal{N}$.

The existence theorem can be deduced by the *local reciprocity law* which says that, for every finite Galois extension L/K of local fields we have a canonical isomorphism

$$\hat{r}_{L/K} : G(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^*/N_{L/K}L^*.$$

In this note, we employ Neukirch's method [4] for the construction of the reciprocity map $\hat{r}_{L/K}$. For the cohomology version of this construction, we recommend Serre's presentation [5].

Most of the theorems in this note are followed by a "sketch of proof" rather than a complete proof. Frequently all the major steps of a proof will be stated, with the reasons or the routine calculational details left to the reader.

Prerequisite for reading this note, apart from Galois theory, is merely a standard introduction to the theory of local fields. We recommend [1, 5] for these subjects.

Lecture notes for a summer school held by NCTS in 2006.

1. Notations and Preliminary Results

A local field is a field which is complete with respect to a discrete valuation, and which has a finite residue class field. These are precisely the finite extensions K of the field $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. We will use the following notation.

- v_K is the discrete valuation normalized by $v_K(K^*) = \mathbb{Z}$.
- $\mathcal{O}_K = \{a \in K \mid v_K(a) \geq 0\}$ is the valuation ring.
- $\mathfrak{P}_K = \{a \in K \mid v_K(a) > 0\}$ is the maximal ideal.
- $U_K = \{a \in K \mid v_K(a) = 0\}$ is the unit group.
- $U_K^{(n)} = \{a \in K \mid v_K(a-1) \geq n\}$
- π_K is a prime element, i.e., $\mathfrak{P}_K = \pi_K \mathcal{O}_K$.
- $\widetilde{K}$ is the maximal unramified extension of K.

Furthermore, for a finite extension L/K,

- $L_0 = L \cap \widetilde{K}$ is the maximal unramified subextension of L/K,
- $e_{L/K} = v_L(\pi_K) = [L : L_0]$ and
- $f_{L/K} = [\mathcal{O}_L/\mathfrak{P}_L : \mathcal{O}_K/\mathfrak{P}_K] = [L_0 : K]$.

We remark that K is locally compact with respect to the discrete valuation topology, and the ring of integers $\mathcal{O}_K$ and the maximal ideal $\mathfrak{P}_K$ are compact. The multiplicative group K^* is also locally compact, and the unit group U_K is compact.

1.1. The residue class field of $\widetilde{K}$ is the algebraic closure $\overline{k}$ of the residue class field k of K. We get a canonical isomorphism

$$G(\widetilde{K}/K) \simeq G(\overline{k}/k).$$

Suppose that $k \simeq \mathbb{F}_q$. This isomorphism associates to the Frobenius automorphism $x \mapsto x^q$ in $G(\overline{k}/k)$ and the Frobenius automorphism ϕ_K in $G(\widetilde{K}/K)$ which is given by

$$a^{\phi_K} \equiv a^q \pmod{\mathfrak{P}_{\widetilde{K}}}, \quad a \in \mathcal{O}_{\widetilde{K}}.$$

The subgroup $\langle \phi_K \rangle = \{\phi_K^n \mid n \in \mathbb{Z}\}$ has the same fixed field K as the whole group $G(\widetilde{K}/K)$. But contrary to what we are used to in finite Galois theory, we find $\langle \phi_K \rangle \neq G(\widetilde{K}/K)$. In fact, there are more subgroups than fixed fields for infinite extension. In order to explain this, let us consider the extension $\overline{\mathbb{F}}_q/\mathbb{F}_q$. Observe first that $\overline{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m \mid n$. Let ϕ be the Frobenius automorphism in $G(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Since $\phi|_{\mathbb{F}_{q^m}}$ has order m, if $a \equiv b \pmod{m}$ then $\phi^a|_{\mathbb{F}_{q^m}} = \phi^b|_{\mathbb{F}_{q^m}}$. Therefore, if we choose a sequence $\{a_n\}_{n\in\mathbb{N}}$ of

integers satisfying $a_n \equiv a_m \pmod{m}$ whenever $m \mid n$, then the map ψ satisfying $\psi|_{\mathbb{F}_{q^m}} = \phi^{a_m}|_{\mathbb{F}_{q^m}}$ is an automorphism of $\overline{\mathbb{F}}_q$. In particular, if we choose $\{a_n\}_{n\in\mathbb{N}}$ such that there is no integer a satisfying $a_n \equiv a \pmod{n}$ for all $n \in \mathbb{N}$, then ψ cannot belong to $\langle\phi\rangle$. In fact, passing from the isomorphism $G(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$ to the projective limit gives an isomorphism

$$G(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

and what we did amounted to writing down the element $(\dots, a_n, \dots) \in \widehat{\mathbb{Z}}$. The projective limit $\widehat{\mathbb{Z}}$ is going to occupy quite an important position in what follows. It contains $\mathbb{Z}$ as a dense subgroup (by considering $\widehat{\mathbb{Z}}$ as the subset of $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ which is equipped with the product topology). The groups $n\widehat{\mathbb{Z}}$, $n \in \mathbb{N}$, are precisely the open subgroups of $\widehat{\mathbb{Z}}$, and it is easy to verify that

$$\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}.$$

The Galois group $G(\Omega/K)$ of any Galois extension Ω/K carries a canonical topology. This topology is called the *Krull topology* and is obtained as follows. for every $\sigma \in G(\Omega/K)$, we take the cosets $\sigma G(\Omega/L)$ as a basis of neighborhoods of σ, with L/K ranging over finite Galois subextensions of Ω/K. The main theorem of Galois theory for infinite extensions can now be formulated as follows.

Theorem 1.1.1. *Let Ω/K be a Galois extension. Then the assignment $M \mapsto G(\Omega/M)$ is a 1-1-correspondence between the subextensions M/K of Ω/K and the closed subgroups of $G(\Omega/K)$.*

In particular, if $\sigma \in G(\Omega/K)$ and Σ is the fixed field of σ, then $G(\Omega/\Sigma)$ is the closure $\overline{\langle\sigma\rangle}$ of the subgroup $\langle\sigma\rangle$. $G(\Omega/\Sigma)$ is a quotient of the group $\widehat{\mathbb{Z}}$. In fact, we have for every n the projective homomorphism

$$\mathbb{Z}/n\mathbb{Z} \to G(\Omega/\Sigma)/G(\Omega/\Sigma)^n, \quad 1 \pmod{n\mathbb{Z}} \mapsto \sigma \pmod{G(\Omega/\Sigma)^n},$$

and passing to the projective limit yields a continuous surjection $\widehat{\mathbb{Z}} \to G(\Omega/\Sigma)$.

1.2. Let G be a finite group and A a (multiplicative) G-module. At the center of class field theory, there are two groups

$$H^0(G, A) = A^G/N_G A \quad \text{and} \quad H^{-1}(G, A) = {}_{N_G}A/I_G A,$$

where

$$A^G = \{a \in A \mid a^\sigma = a, \forall\, \sigma \in G\}, \quad N_G A = \{N_G a = \prod_{\sigma\in G} a^\sigma \mid a \in A\},$$

$$ {}_{N_G}A = \{a \in A \mid N_G a = 1\} $$

and $I_G A$ is the subgroup of ${}_{N_G}A$ which is generated by all elements $a^{\sigma-1}$, with $a \in A$ and $\sigma \in G$.

We will be mainly interested in the case where G is a finite cyclic group. If G is cyclic and σ is a generator, then $I_G A$ is simply the group $A^{\sigma-1} = \{a^{\sigma-1} \mid a \in A\}$. In fact, the formal identity $\sigma^m - 1 = (1+\sigma+\cdots+\sigma^{m-1})(\sigma-1)$ implies $a^{\sigma^m-1} = b^{\sigma-1}$ with $b = \prod_{i=0}^{m-1} a^{\sigma^i}$.

Suppose that G is a finite cyclic group. If $1 \to A \to B \to C \to 1$ is an exact sequence of G-modules, then we obtain an *exact hexagon*

$$ \begin{array}{ccccc} & & H^0(G,A) & \longrightarrow & H^0(G,B) & & \\ & \nearrow & & & & \searrow & \\ H^{-1}(G,C) & & & & & & H^0(G,C) \\ & \nwarrow & & & & \swarrow & \\ & & H^{-1}(G,B) & \longleftarrow & H^{-1}(G,A) & & \end{array} $$

An excellent tool for studying $H^0(G,A)$ and $H^{-1}(G,A)$ is the *Herbrand quotient*. The Herbrand quotient of the G-module A is defined to be

$$ h(G,A) = \frac{\#H^0(G,A)}{\#H^{-1}(G,A)}, $$

provided that both orders are finite. In particular, if $G = \langle\sigma\rangle$ and A is a finite G-module, then the exact sequences

$$ 1 \longrightarrow A^G \longrightarrow A \xrightarrow{\sigma-1} I_G A \longrightarrow 1 \quad \text{and} \quad 1 \longrightarrow {}_{N_G}A \longrightarrow A \xrightarrow{N_G} N_G A \longrightarrow 1, $$

show that $\#A = \#A^G \cdot \#I_G A = \#\,{}_{N_G}A \cdot \#N_G A$, and hence $h(G,A) = 1$.

Using the exact hexagon, we can deduce the *multiplicativity* of the Herbrand quotient.

Proposition 1.2.1. *Let G be a finite cyclic group. If $1 \to A \to B \to C \to 1$ is an exact sequence of G-modules, then one has*

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

in the sense that, whenever two of these quotients are defined, so is the third and the identity holds.

In local class field theory, the crucial point is to verify for the multiplicative group of a local field the *class field axiom*:

Theorem 1.2.2. *For a cyclic extension L/K of local fields, one has*

$$ \#H^0(G(L/K), L^*) = [L:K] \quad \text{and} \quad \#H^{-1}(G(L/K), L^*) = 1. $$

Proof. For $\#H^{-1}(G(L/K), L^*) = 1$, this is the famous "Hilbert 90". So all we have to show is that the Herbrand quotient is $h(G, L^*) = H^0(G, L^*) = [L : K]$, where we have put $G = G(L/K)$. The exact sequence $1 \to U_L \to L^* \xrightarrow{v_L} \mathbb{Z} \to 0$, in which $\mathbb{Z}$ has to be viewed as the trivial G-module, yields, by Proposition 1.2.1,

$$h(G, L^*) = h(G, U_L)h(G, \mathbb{Z}) = h(G, U_L)[L : K].$$

Hence we have to show that $h(G, U_L) = 1$.

First, we choose a normal basis $\{\alpha^\sigma \mid \sigma \in G\}$ of L/K with $\alpha \in \mathcal{O}_L$ (see [2, Chapter VIII]), and consider the open G-module $M = \sum_{\sigma\in G} \mathcal{O}_K \alpha^\sigma$. Then consider the open sets

$$V^n = 1 + \pi_K^n M,\ n \in \mathbb{N}.$$

Since M is open, we have $\pi_K^N \mathcal{O}_L \subseteq M$ for suitable N, and for $n \geq N$ the V^n are subgroups of U_L. Via the correspondence $1 + \pi_K^n \beta \mapsto \beta \pmod{\pi_K M}$, we obtain G-isomorphisms

$$V^n/V^{n+1} \simeq M/\pi_K M = \bigoplus_{\sigma\in G} (\mathcal{O}_K/\mathfrak{P}_K)\alpha^\sigma.$$

It is easy to check that

$$H^0(G, \bigoplus_{\sigma\in G} (\mathcal{O}_K/\mathfrak{P}_K)\alpha^\sigma) = H^{-1}(G, \bigoplus_{\sigma\in G} (\mathcal{O}_K/\mathfrak{P}_K)\alpha^\sigma) = 0,$$

and hence

$$H^0(G, V^n/V^{n+1}) = H^{-1}(G, V^n/V^{n+1}) = 1, \quad \text{for } n \geq N.$$

This implies that $H^0(G, V^n) = 1$, for $n \geq N$. Indeed, if $a \in (V^n)^G$, then $a = (N_G b_0)a_1$, with $b_0 \in V^n$ and $a_1 \in (V^{n+1})^G$. Continuing in this way, by the completeness yields $a = N_G b$, with $b = \prod_{i=0}^\infty b_i \in V^n$, so that $H^0(G, V^n) = 1$. Similarly, we have $H^{-1}(G, V^n) = 1$, for $n \geq N$. Because U_L is compact, U_L/V^n is finite. Therefore, by Proposition 1.2.1, we obtain

$$h(G, U_L) = h(G, U_L/V^n)h(G, V^n) = 1.$$

□

Among the cyclic extensions there are in particular the unramified extensions, so that one has

Corollary 1.2.3. *For a finite unramified extension L/K, one has*

$$H^0(G(L/K), U_L) = H^{-1}(G(L/K), U_L) = 1$$

and

$$H^0(G(L/K), U_L^{(n)}) = H^{-1}(G(L/K), U_L^{(n)}) = 1, \quad n \in \mathbb{N}.$$

Proof. Let $G = G(L/K)$. As $H^{-1}(G, L^*) = 1$, every element $u \in U_L$ such that $N_{L/K}(u) = 1$ is of the form $u = a^{\phi_{L/K}-1}$, with $a \in L^*$ and $\phi_{L/K} = \phi_K|_L$. Since L/K is unramified, π_K is also a prime element of L. So writing $a = \varepsilon\pi_K^m$ with $\varepsilon \in U_L$, we obtain $u = \varepsilon^{\phi_{L/K}-1}$. This shows that $H^{-1}(G, U_L) = 1$. Since we have proved that $h(G, U_L) = 1$ in Theorem 1.2.2, this shows that $H^0(G, U_L) = 1$.

In order to prove $H^0(G, U_L^{(n)}) = H^{-1}(G, U_L^{(n)}) = 1$, we first show that

$$H^0(G, l^*) = H^{-1}(G, l^*) = 1 \quad \text{and} \quad H^0(G, l) = H^{-1}(G, l) = 0,$$

for the residue class field l of L. We have $H^{-1}(G, l^*) = 1$ by Hilbert 90. This implies that $H^0(G, l^*) = 1$, as l is finite and so $h(G, l^*) = 1$. Let $f = [l : k]$ be the degree of l over the residue class field k of K, and let $q = \#k$. Then we have

$$\#\,{}_{N_G} l = \#\{x \in l \mid \sum_{i=0}^{f-1} x^{q^i} = 0\} \leq q^{f-1} \quad \text{and} \quad \#I_G l = q^{f-1},$$

since k is the fixed field of the Frobenius automorphism $l \xrightarrow{\uparrow q} l$. Therefore

$$H^{-1}(G, l) = {}_{N_G} l / I_G l = 0.$$

This implies that $H^0(G, l) = 0$ as $h(G, l) = 1$.

Applying now the exact hexagon to the exact sequence of G-modules

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

we obtain

$$H^0(G, U_L^{(1)}) = H^0(G, U_L) = 1 \quad \text{and} \quad H^{-1}(G, U_L^{(1)}) = H^{-1}(G, U_L) = 1.$$

From the exact sequence of G-modules

$$1 \to U_L^{(n+1)} \to U_L^{(n)} \to l \to 0,$$

we now deduce by induction just as above, that

$$H^0(G, U_L^{(n+1)}) = H^0(G, U_L^{(n)}) = 1 \quad \text{and} \quad H^{-1}(G, U_L^{(n+1)}) = H^{-1}(G, U_L^{(n)}) = 1.$$

□

2. The Local Reciprocity Law

The Frobenius automorphism governs the entire class field theory like a king. It is therefore most remarkable that in the case of a finite Galois extension L/K, every $\sigma \in G(L/K)$ becomes a Frobenius automorphism once it is maneuvered into the right position. This point of view helps us to construct the reciprocity map which expresses the fundamental principle of class field theory to the effect that Frobenius automorphisms correspond to prime elements.

2.1. For a local field K, we denote by ϕ_K the Frobenius automorphism in $G(\widetilde{K}/K)$. Let $d_K : G(\widetilde{K}/K) \to \widehat{\mathbb{Z}}$ be the isomorphism such that $d_K(\phi_K) = 1$. We pass from the Galois extension L/K to the extension $\widetilde{L}/K$ and consider the function $d_{L/K} : G(\widetilde{L}/K) \to \widehat{\mathbb{Z}}$ such that $d_{L/K}(\sigma) = d_K(\sigma|_{\widetilde{K}})$, for $\sigma \in G(\widetilde{L}/K)$. In particular, since $\phi_L|_{\widetilde{K}} = \phi_K^{f_{L/K}}$, one has $d_{L/K}(\phi_L) = f_{L/K}$. Notice that every element in $G(\widetilde{K}/K)$ can be extended to an element in $G(\widetilde{L}/K)$. Therefore, $d_{L/K} : G(\widetilde{L}/K) \to \widehat{\mathbb{Z}}$ is surjective.

Consider in the Galois group $G(\widetilde{L}/K)$ the semigroup

$$\mathrm{Frob}(\widetilde{L}/K) = \{\sigma \in G(\widetilde{L}/K) \mid d_{L/K}(\sigma) \in \mathbb{N}\}.$$

In other words, $\sigma \in \mathrm{Frob}(\widetilde{L}/K)$ if and only if $\sigma \in G(\widetilde{L}/K)$ and $\sigma|_{\widetilde{K}} = \phi_K^n$, for some $n \in \mathbb{N}$. Because $d_{L/K}(1) = 0$ and $d_{L/K}(\sigma_1\sigma_2) = d_{L/K}(\sigma_1) + d_{L/K}(\sigma_2)$, one knows that $1 \notin \mathrm{Frob}(\widetilde{L}/K)$ and $\mathrm{Frob}(\widetilde{L}/K)$ is closed with respect to multiplication (but not closed with respect to inversion). Moreover, since $d_{L/K}$ is surjective, $d_{L/K}$ maps $\mathrm{Frob}(\widetilde{L}/K)$ onto $\mathbb{N}$. Firstly, we have the

Proposition 2.1.1. *For a finite Galois extension L/K, the mapping*

$$\mathrm{Frob}(\widetilde{L}/K) \to G(L/K), \quad \sigma \mapsto \sigma|_L,$$

is surjective.

Proof. Let $\tilde{\phi} \in \mathrm{Frob}(\widetilde{L}/K)$ be an element such that $d_{L/K}(\tilde{\phi}) = 1$. Then $\tilde{\phi}|_{\widetilde{K}} = \phi_K$. Remark here that $L_0 = L \cap \widetilde{K}$ is the maximal unramified subextension of L/K. For $\rho \in G(L/K)$, since $\rho|_{L_0} \in G(L_0/K) = \langle \tilde{\phi}|_{L_0} \rangle$, there exists $n \in \mathbb{N}$ such that $\rho|_{L_0} = \tilde{\phi}^n|_{L_0}$. Since $\rho\tilde{\phi}^{-n}|_L \in G(L/L_0)$ and the mapping

$$G(\widetilde{L}/\widetilde{K}) \to G(L/L_0), \quad \tau \mapsto \tau|_L$$

is an isomorphism, there is $\tau \in G(\widetilde{L}/\widetilde{K})$ such that $\tau|_L = \rho\tilde{\phi}^{-n}|_L$. Therefore, $\sigma = \tau\tilde{\phi}^n \in G(\widetilde{L}/K)$ is an element satisfying $\sigma \in \mathrm{Frob}(\widetilde{L}/K)$ (because $\sigma|_{\widetilde{K}} = \phi_K^n$) such that $\sigma|_L = \tau\tilde{\phi}^n|_L = \rho$. □

Thus every element $\sigma \in G(L/K)$ may be lifted to an element in $\mathrm{Frob}(\widetilde{L}/K)$. The following proposition shows that this lifting, considered over its fixed field, is actually the Frobenius automorphism.

Proposition 2.1.2. *Let $\sigma \in \mathrm{Frob}(\widetilde{L}/K)$ and let Σ be the fixed field of σ. Then Σ/K is a finite extension such that $\widetilde{\Sigma} = \widetilde{L}$, $f_{\Sigma/K} = d_{L/K}(\sigma)$ and $e_{\Sigma/K} = e_{L/K}$. Moreover, $\sigma = \phi_\Sigma$.*

Proof. We first show that $\widetilde{\Sigma} = \widetilde{L}$. Since $\Sigma \subseteq \widetilde{L}$, one has $\widetilde{\Sigma} \subseteq \widetilde{L}$. The canonical surjection $G(\widetilde{L}/\Sigma) \to G(\widetilde{\Sigma}/\Sigma)$, $\tau \mapsto \tau|_{\widetilde{\Sigma}}$ must be bijective, because $G(\widetilde{L}/\Sigma) = \overline{\langle\sigma\rangle}$ is a quotient of $\widehat{\mathbb{Z}} \simeq G(\widetilde{\Sigma}/\Sigma)$. But $G(\widetilde{L}/\Sigma) = G(\widetilde{\Sigma}/\Sigma)$ implies that $\widetilde{\Sigma} = \widetilde{L}$. This also implies that $e_{\Sigma/K} = [\widetilde{\Sigma} : \widetilde{K}] = [\widetilde{L} : \widetilde{K}] = e_{L/K}$.

Suppose that $d_{L/K}(\sigma) = d$. In other words, $\sigma|_{\widetilde{K}} = \phi_K^d$. Because the fixed field of $\sigma|_{\widetilde{K}}$ is $\Sigma \cap \widetilde{K} = \Sigma_0$, we have $f_{\Sigma/K} = [\Sigma_0 : K] = d$. Therefore,

$$[\Sigma : K] = e_{\Sigma/K} f_{\Sigma/K} = e_{L/K} d \leq [L : K] d_{L/K}(\sigma)$$

is finite.

Finally, since $f_{\Sigma/K} = [\Sigma_0 : K] = d$, one has $\phi_\Sigma|_{\widetilde{K}} = \phi_K^d = \sigma|_{\widetilde{K}}$. Hence, $\sigma \in G(\widetilde{\Sigma}/\Sigma)$ and $\phi_\Sigma \in G(\widetilde{\Sigma}/\Sigma)$ are identical in $\Sigma\widetilde{K} = \widetilde{\Sigma}$. Thus $\sigma = \phi_\Sigma$. □

Our goal is to define a canonical homomorphism

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

for every finite Galois extension L/K. To this end, we define first a mapping on $\mathrm{Frob}(\widetilde{L}/K)$.

Definition 2.1.3. The *reciprocity map*

$$r_{\widetilde{L}/K} : \mathrm{Frob}(\widetilde{L}/K) \to K^*/N_{L/K}L^*$$

is defined by

$$r_{\widetilde{L}/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \pmod{N_{L/K}L^*},$$

where Σ is the fixed field of σ.

Observe that the definition of $r_{\widetilde{L}/K}(\sigma)$ does not depend on the choice of the element π_Σ. For another prime element differs from π_Σ only by an element $u \in U_\Sigma$,

and for this we have $N_{\Sigma/K}(u) \in N_{L/K}L^*$. To see this, we let $M = L\Sigma$. Applying Corollary 1.2.3 to the unramified extension M/Σ (because $\widetilde{M} = \widetilde{\Sigma}$), one finds $u = N_{M/\Sigma}(\varepsilon)$, for some $\varepsilon \in U_M$, and thus

$$N_{\Sigma/K}(u) = N_{\Sigma/K}(N_{M/\Sigma}(\varepsilon)) = N_{L/K}(N_{M/L}(\varepsilon)) \in N_{L/K}L^*.$$

Next we want to show that the reciprocity map $r_{\widetilde{L}/K}$ is multiplicative. In other words, we have to show that if $\sigma_1\sigma_2 = \sigma_3$ is an equation in $\mathrm{Frob}(\widetilde{L}/K)$ and Σ_i the fixed field of σ_i, for $i = 1, 2, 3$, then

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

To do this, we need two Lemmas.

Our first lemma makes $N_{\Sigma_i/K}(\pi_{\Sigma_i})$, for $i = 1, 2, 3$ as a norm over the same fields.

Lemma 2.1.4. *For a finite Galois extension L/K, let $\phi, \sigma \in \mathrm{Frob}(\widetilde{L}/K)$ with $d_{L/K}(\phi) = 1$ and $d_{L/K}(\sigma) = n$. If Σ is the fixed field of σ and $a \in \Sigma$, then*

$$N_{\Sigma/K}(a) = N_{\widetilde{L}/\widetilde{K}}(\prod_{i=0}^{n-1} a^{\phi^i}).$$

Proof. Since $\widetilde{\Sigma} = \widetilde{L}$ (Proposition 2.1.2), for $a \in \Sigma$ we have $N_{\Sigma/\Sigma_0}(a) = N_{\widetilde{\Sigma}/\widetilde{K}}(a) = N_{\widetilde{L}/\widetilde{K}}(a)$. On the other hand, since $[\Sigma_0 : K] = f_{\Sigma/K} = n$ and $G(\Sigma_0/K)$ is generated by $\phi_K|_{\Sigma_0} = \phi|_{\Sigma_0}$, one has $N_{\Sigma_0/K}(b) = \prod_{i=0}^{n-1} b^{\phi^i}$, for $b \in \Sigma_0$. For $a \in \Sigma$ we thus get

$$N_{\Sigma/K}(a) = N_{\Sigma_0/K}(N_{\Sigma/\Sigma_0}(a)) = \prod_{i=0}^{n-1} N_{\widetilde{L}/\widetilde{K}}(a)^{\phi^i} = N_{\widetilde{L}/\widetilde{K}}(\prod_{i=0}^{n-1} a^{\phi^i}).$$

The last equation follows from $\phi G(\widetilde{L}/\widetilde{K}) = G(\widetilde{L}/\widetilde{K})\phi$. □

Next lemma provide us a method to identify an element which is in $N_{L/K}L^*$.

Lemma 2.1.5. *For a finite Galois extension L/K, let $\phi \in \mathrm{Frob}(\widetilde{L}/K)$ satisfy $d_{L/K}(\phi) = 1$. Suppose that $u \in U_{\widetilde{L}}$ such that $u^{\phi-1} = \prod_{i=1}^{r} u_i^{\tau_i - 1}$, for some $u_i \in U_{\widetilde{L}}$ and $\tau_i \in G(\widetilde{L}/\widetilde{K})$. Then $N_{\widetilde{L}/\widetilde{K}}(u) \in N_{L/K}L^*$.*

Proof. Let M/K be a finite Galois subextension of $\widetilde{L}/K$ such that $u, u_i \in U_M$ and $L \subseteq M$. Let $[M : K] = n$, $\sigma = \phi^n$ and let Σ be the fixed field of σ. Since $\widetilde{M} = \widetilde{\Sigma}$ and $f_{M/K} \mid n = f_{\Sigma/K}$, we have that $M \subseteq \Sigma$. Further, let Σ'/Σ be the unramified extension of degree n. By Corollary 1.2.3, we can then find elements $\tilde{u}, \tilde{u}_i \in U_{\Sigma'}$ such that $u = N_{\Sigma'/\Sigma}(\tilde{u})$ and $u_i = N_{\Sigma'/\Sigma}(\tilde{u}_i)$. Since $G(\Sigma'/\Sigma)$ is generated by $\sigma|_{\Sigma'} = \phi_\Sigma|_{\Sigma'}$ and $\phi G(\widetilde{L}/\widetilde{K}) = G(\widetilde{L}/\widetilde{K})\phi$, by the assumption we have $\tilde{u}^{\phi-1} = \lambda \prod_{i=1}^{r} \tilde{u}_i^{\tau_i - 1}$, for

an element $\lambda \in U_{\Sigma'}$ such that $N_{\Sigma'/\Sigma}(\lambda) = 1$. Hence, again by Corollary 1.2.3, $\lambda = \mu^{\sigma-1} = \mu^{\phi^n-1}$, with $\mu \in U_{\Sigma'}$. We may thus write

$$\tilde{u}^{\phi-1} = \mu^{\phi^n-1} \prod_{i=1}^{r} \tilde{u}_i^{\tau_i-1} = (\prod_{j=1}^{n-1} \mu^{\phi^j})^{\phi-1} \prod_{i=1}^{r} \tilde{u}_i^{\tau_i-1}.$$

Applying $N_{\widetilde{L}/\widetilde{K}}$ gives $N_{\widetilde{L}/\widetilde{K}}(\tilde{u})^{\phi-1} = N_{\widetilde{L}/\widetilde{K}}(\prod_{j=1}^{n-1} \mu^{\phi^j})^{\phi-1}$, so that

$$N_{\widetilde{L}/\widetilde{K}}(\tilde{u}) = N_{\widetilde{L}/\widetilde{K}}(\prod_{j=1}^{n-1} \mu^{\phi^j})z,$$

for some $z \in U_K$. Finally, applying $N_{\Sigma'/\Sigma}$, we obtain, observing $n = [M : K] = [\Sigma' : \Sigma]$ and using Lemma 2.1.4, that

$$\begin{aligned} N_{\widetilde{L}/\widetilde{K}}(u) &= N_{\widetilde{L}/\widetilde{K}}(N_{\Sigma'/\Sigma}(\tilde{u})) = N_{\Sigma'/\Sigma}(N_{\widetilde{L}/\widetilde{K}}(\tilde{u})) = N_{\Sigma'/\Sigma}(N_{\widetilde{L}/\widetilde{K}}(\prod_{j=1}^{n-1} \mu^{\phi^j}))z^n \\ &= N_{\widetilde{L}/\widetilde{K}}(\prod_{j=1}^{n-1} N_{\Sigma'/\Sigma}(\mu)^{\phi^j})z^n = N_{\Sigma/K}(N_{\Sigma'/\Sigma}(\mu))N_{M/K}(z) \in N_{L/K}L^*. \end{aligned}$$

□

Now we are ready to show the

Proposition 2.1.6. *For a finite Galois extension L/K, the reciprocity map is multiplicative.*

Proof. Let $\sigma_1\sigma_2 = \sigma_3$ be an equation in $\mathrm{Frob}(\widetilde{L}/K)$, Σ_i the fixed field of σ_i and $\pi_i = \pi_{\Sigma_i}$, for $i = 1, 2, 3$. We have to show that

$$N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \equiv N_{\Sigma_3/K}(\pi_3) \pmod{N_{L/K}L^*}.$$

Suppose that $d_{L/K}(\sigma_i) = n_i$, for $i = 1, 2, 3$. In order to apply Lemma 2.1.5, we choose a fixed $\phi \in \mathrm{Frob}(\widetilde{L}/K)$ such that $d_{L/K}(\phi) = 1$ and put

$$\tau_i = \sigma_i^{-1}\phi^{n_i} \in G(\widetilde{L}/\widetilde{K}), \quad i = 1, 2, 3.$$

From $\sigma_1\sigma_2 = \sigma_3$ and $n_1 + n_2 = n_3$, we then deduce that $\tau_3 = \tau_2(\phi^{-n_2}\sigma_1\phi^{n_2})^{-1}\phi^{n_1}$. Putting $\sigma_4 = \phi^{-n_2}\sigma_1\phi^{n_2}$ and $n_4 = d_{L/K}(\sigma_4) = n_1$ and $\tau_4 = \sigma_4^{-1}\phi^{n_4}$, we find that $\tau_3 = \tau_2\tau_4$ and $N_{\Sigma_4/K}(\pi_4) = N_{\Sigma_1/K}(\pi_1)$, where $\Sigma_4 = \Sigma_1^{\phi^{n_2}}$ is the fixed field of σ_4 and $\pi_4 = \pi_1^{\phi^{n_2}}$ is a prime element of Σ_4. We may therefore pass to show the congruence

$$N_{\Sigma_2/K}(\pi_2)N_{\Sigma_4/K}(\pi_4) \equiv N_{\Sigma_3/K}(\pi_3) \pmod{N_{L/K}L^*}.$$

From Lemma 2.1.4, if we put

$$u = \Big(\prod_{i=0}^{n_2-1} \pi_2^{\phi^i}\Big)\Big(\prod_{i=0}^{n_4-1} \pi_4^{\phi^i}\Big)\Big(\prod_{i=0}^{n_3-1} (\pi_3^{-1})^{\phi^i}\Big) \in U_{\widetilde{L}},$$

then the congruence amounts simply to the relation $N_{\widetilde{L}/\widetilde{K}}(u) \in N_{L/K}L^*$. For this, however, Lemma 2.1.5 gives us all that we need.

Since σ_i fixes π_i, we have $\pi_i^{\phi^{n_i}-1} = \pi_i^{\sigma_i^{-1}\phi^{n_i}-1} = \pi_i^{\tau_i-1}$, and hence $u^{\phi-1} = \pi_2^{\tau_2-1}\pi_4^{\tau_4-1}\pi_3^{1-\tau_3}$. Because $\widetilde{\Sigma}_2 = \widetilde{\Sigma}_3 = \widetilde{\Sigma}_4$, we have $\pi_2 = u_2\pi_4$, $\pi_3 = u_3^{-1}\pi_4$ and $\pi_4^{\tau_2} = u_4^{-1}\pi_4$, for $u_2, u_3, u_4 \in U_{\widetilde{L}}$. We obtain $u^{\phi-1} = u_2^{\tau_2-1}u_3^{\tau_3-1}u_4^{\tau_4-1}$. By Lemma 2.1.5, we do get $N_{\widetilde{L}/\widetilde{K}}(u) \in N_{L/K}L^*$. □

2.2. From the surjectivity of the mapping $\mathrm{Frob}(\widetilde{L}/K) \to G(L/K)$, we now have the

Proposition 2.2.1. *For every finite Galois extension L/K, there is a canonical homomorphism $r_{L/K} : G(L/K) \to K^*/N_{L/K}L^*$ given by*

$$r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \pmod{N_{L/K}L^*},$$

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

Proof. We first show that the definition of $r_{L/K}$ is independent of the choice of the extension $\tilde{\sigma} \in \mathrm{Frob}(\widetilde{L}/K)$ of $\sigma \in G(L/K)$. For this, let $\tilde{\sigma}' \in \mathrm{Frob}(\widetilde{L}/K)$ be another extension and Σ' its fixed field. If $d_{L/K}(\tilde{\sigma}) = d_{L/K}(\tilde{\sigma}')$, then $\tilde{\sigma}|_{\widetilde{K}} = \tilde{\sigma}'|_{\widetilde{K}}$ and $\tilde{\sigma}|_L = \tilde{\sigma}'|_L$, so that $\tilde{\sigma} = \tilde{\sigma}'$, and there is nothing to show. However, if we have, say, $d_{L/K}(\tilde{\sigma}) < d_{L/K}(\tilde{\sigma}')$, then denote $\tau = \tilde{\sigma}^{-1}\tilde{\sigma}'$. The automorphism $\tau \in G(\widetilde{L}/L)$ and $d_{L/K}(\tau) = d_{L/K}(\tilde{\sigma}') - d_{L/K}(\tilde{\sigma}) \in \mathbb{N}$. Hence $\tau \in \mathrm{Frob}(\widetilde{L}/K)$ and the fixed field Σ'' of τ contains L. Therefore, Proposition 2.1.6 shows that

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

This means that $r_{L/K}$ is well defined.

The fact that the mapping is a homomorphism follows directly from Proposition 2.1.6. □

Definition 2.2.2. The *reciprocity homomorphism*

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

is defined by

$$r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \pmod{N_{L/K}L^*},$$

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

The definition of the reciprocity map expresses the fundamental principle of class field theory to the effect that Frobenius automorphisms correspond to prime elements. This principle appears at its purest in the

Proposition 2.2.3. *If L/K is a finite unramified extension, then the reciprocity homomorphism $r_{L/K} : G(L/K) \to K^*/N_{L/K}L^*$ is given by*

$$r_{L/K}(\phi_K|_L) \equiv \pi_K \pmod{N_{L/K}L^*}$$

and is an isomorphism.

Proof. In this case $\widetilde{L} = \widetilde{K}$, the Frobenius automorphism $\phi_K \in \mathrm{Frob}(\widetilde{L}/K)$ is an extension of $\phi_K|_L$. The fixed filed of ϕ_K is K, and hence by definition, $r_{L/K}(\phi_K|_L) \equiv \pi_K \pmod{N_{L/K}L^*}$.

Consider the valuation map $v_K : K^* \to \mathbb{Z}$. It induces an isomorphism

$$K^*/N_{L/K}L^* \simeq \mathbb{Z}/n\mathbb{Z},$$

with $n = [L : K]$. Indeed, if $v_K(a) \equiv 0 \pmod{n\mathbb{Z}}$, then $a = u\pi_K^{nr}$, and since $u = N_{L/K}(\varepsilon)$ for some $\varepsilon \in U_L$ (Corollary 1.2.3), we find $a = N_{L/K}(\varepsilon\pi_K^r) \equiv 1 \pmod{N_{L/K}L^*}$. This shows that $\pi_K \pmod{N_{L/K}L^*}$ generates the cyclic group $K^*/N_{L/K}L^*$ of order $[L : K]$. Since $\phi_K|_L$ also generates the cyclic group $G(L/K)$, we have $r_{L/K}$ is an isomorphism. □

The homomorphism $r_{L/K}$ in general is not an isomorphism. This can be clearly seen when $G(L/K)$ is not abelian. Finite unramified extension is always a cyclic extension. Next, we treat the other extreme case.

Proposition 2.2.4. *If L/K is a finite extension which is cyclic and totally ramified, then the reciprocity homomorphism $r_{L/K} : G(L/K) \to K^*/N_{L/K}L^*$ is an isomorphism.*

Proof. Since L/K is totally ramified, we have an isomorphism $G(\widetilde{L}/\widetilde{K}) \to G(L/K)$ given by restriction. Let $\tilde{\sigma} \in G(\widetilde{L}/\widetilde{K})$ be a generator. Then $\sigma = \tilde{\sigma}|_L$ is a generator of $G(L/K)$. Let $\sigma_1 = \tilde{\sigma}\phi_L \in G(\widetilde{L}/K)$. Since

$$d_{L/K}(\sigma_1) = d_K(\sigma_1|_{\widetilde{K}}) = d_K(\phi_L|_{\widetilde{K}}) = f_{L/K} = 1$$

and $\sigma_1|_L = \tilde{\sigma}|_L = \sigma$, we have that $\sigma_1 \in \mathrm{Frob}(\widetilde{L}/K)$ is an extension of σ. We thus find for the fixed field Σ/K of σ_1 that $f_{\Sigma/K} = d_{L/K}(\sigma_1) = 1$ (Proposition 2.1.2), and so $\Sigma_0 = \Sigma \cap \widetilde{K} = K$. Let M/K be a finite Galois subextension of

$\widetilde{L}/K$ containing Σ and L and let $M_0 = M \cap \widetilde{K}$. Since $\widetilde{M} = \widetilde{\Sigma} = \widetilde{L}$, we have that $G(M/M_0) \simeq G(\Sigma/K) \simeq G(L/K)$ and $N_{M/M_0}|_\Sigma = N_{\Sigma/K}$, $N_{M/M_0}|_L = N_{L/K}$.

For the injectivity of $r_{L/K}$, we claim that: if $r_{L/K}(\sigma^m) \equiv 1 \pmod{N_{L/K}L^*}$, where $0 \leq m < n = [L:K]$, then $m = 0$.

Let $\pi_L \in \mathcal{O}_L$ and $\pi_\Sigma \in \mathcal{O}_\Sigma$ be prime elements. Since $\Sigma, L \subseteq M$ and $\widetilde{M} = \widetilde{\Sigma} = \widetilde{L}$, π_L and π_Σ are both prime elements of M. Putting $\pi_\Sigma^m = u\pi_L^m$, with $u \in U_M$, we obtain

$$r_{L/K}(\sigma^m) \equiv N_{\Sigma/K}(\pi_\Sigma^m) \equiv N_{M/M_0}(u) N_{L/K}(\pi_L^m) \equiv N_{M/M_0}(u) \pmod{N_{L/K}L^*}.$$

From $r_{L/K}(\sigma^m) \equiv 1 \pmod{N_{L/K}L^*}$, it thus follows that $N_{M/M_0}(u) = N_{L/K}(\varepsilon)$ for some $\varepsilon \in U_L$. Since $G(M/M_0)$ is cyclic, from Theorem 1.2.2 (Hilbert 90), we may write $u^{-1}\varepsilon = a^{\tilde{\sigma}-1}$ for some $a \in M^*$ and have

$$\begin{aligned} (\pi_L^m \varepsilon)^{\tilde{\sigma}-1} &= (\pi_L^m \varepsilon)^{\sigma_1 - 1} \quad (\text{because } \tilde{\sigma}|_L = \sigma_1|_L) \\ &= (\pi_\Sigma^m \cdot a^{\tilde{\sigma}-1})^{\sigma_1 - 1} \\ &= (a^{\sigma_1 - 1})^{\tilde{\sigma}-1} \end{aligned}$$

Hence we have $b = \pi_L^m \varepsilon a^{1-\sigma_1} \in M_0^*$ with $v_M(b) = m$. However, $v_M(b) = e_{M/M_0} v_{M_0}(b) = n v_{M_0}(b)$ implies that one has $m = 0$, and so $r_{L/K}$ is injective. The surjectivity the follows from Theorem 1.2.2

$$\#K^*/N_{L/K}L^* = [L:K] = \#G(L/K).$$

□

The reciprocity homomorphism $r_{L/K}$ exhibits the following functorial behavior.

Proposition 2.2.5. *Let L/K and L_1/K_1 be finite Galois extensions such that K_1/K and L_1/L are finite separable extensions. Then we have the commutative diagram*

$$\begin{array}{ccc} G(L_1/K_1) & \xrightarrow{r_{L_1/K_1}} & {K_1}^*/N_{L_1/K_1}L_1^* \\ \downarrow{\scriptstyle |_L} & & \downarrow{\scriptstyle N_{K_1/K}} \\ G(L/K) & \xrightarrow{r_{L/K}} & K^*/N_{L/K}L^* \end{array}$$

where the left vertical homomorphism are given by the restriction $\sigma_1|_L$ of $\sigma_1 \in G(L_1/K_1)$ and the right vertical homomorphism is induced by the norm map $N_{K_1/K}$.

Proof. Let $\sigma' \in G(L_1/K_1)$ and $\sigma = \sigma'|_L \in G(L/K)$. If $\tilde{\sigma}' \in \mathrm{Frob}(\widetilde{L}_1/K_1)$ is an extension of σ', then $\tilde{\sigma} = \tilde{\sigma}'|_{\widetilde{L}} \in \mathrm{Frob}(\widetilde{L}/K)$ is an extension of σ, because $d_{L/K}(\tilde{\sigma}) = f_{K_1/K} d_{L_1/K_1}(\tilde{\sigma}') \in \mathbb{N}$. Let Σ' be the fixed field of $\tilde{\sigma}'$. Then the fixed

field of $\tilde{\sigma}$ is $\Sigma = \Sigma' \cap \widetilde{L} = \Sigma' \cap \widetilde{\Sigma} = \Sigma'_0$ and hence $f_{\Sigma'/\Sigma} = [\Sigma'_0 : \Sigma] = 1$. If now $\pi_{\Sigma'}$ is a prime element of Σ', then $\pi_\Sigma = N_{\Sigma'/\Sigma}(\pi_{\Sigma'})$ is a prime element of Σ. The commutativity of the diagram follows from the equality of norms

$$N_{\Sigma/K}(\pi_\Sigma) = N_{\Sigma/K}(N_{\Sigma'/\Sigma}(\pi_{\Sigma'}) = N_{K_1/K}(N_{\Sigma'/K_1}(\pi_{\Sigma'})).$$

□

As an easy consequence of the preceding proposition, we have the

Corollary 2.2.6. *Let M/K be a Galois subextension of a finite Galois extension L/K. Then we have the commutative exact diagram*

$$\begin{array}{ccccccccc} 1 & \to & G(L/M) & \to & G(L/K) & \to & G(M/K) & \to & 1 \\ & & \downarrow{\scriptstyle r_{L/M}} & & \downarrow{\scriptstyle r_{L/K}} & & \downarrow{\scriptstyle r_{M/K}} & & \\ & & M^*/N_{L/M}L^* & \xrightarrow{N_{M/K}} & K^*/N_{L/K}L^* & \to & K^*/N_{M/K}M^* & \to & 1 \end{array} \tag{2.1}$$

where the central homomorphism of the lower sequence is induced by the identity map of K^*.

It is clear that when $G(L/K)$ is not abelian the homomorphism $r_{L/K}$ is not an isomorphism. For an arbitrary group G, let G' denote the commutator subgroup and write $G^{\mathrm{ab}} = G/G'$ for the maximal abelian quotient group. Since $K^*/N_{L/K}L^*$ is an abelian group, the homomorphism $r_{L/K}$ naturally induces the homomorphism

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

which represents the main theorem of class field theory, and which we will call the *Local Reciprocity Law*:

Theorem 2.2.7. *For every finite Galois extension L/K of local fields, we have a canonical isomorphism*

$$\hat{r}_{L/K} : G(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^*/N_{L/K}L^*.$$

Proof. If M/K is a Galois subextension of L/K, we get from Corollary 2.2.6 the commutative exact diagram (2.1). Using this diagram, we will prove this theorem in three steps.

First, we show that $\hat{r}_{L/K} = r_{L/K}$ is an isomorphism for every finite cyclic extension L/K. Let $M = L \cap \widetilde{K}$ in diagram (2.1) be the maximal unramified subextension of L/K. Then L/M is a cyclic totally ramified extension and M/K is a unramified extension. Hence, $r_{M/K}$ and $r_{L/M}$ are isomorphisms by Propositions 2.2.3 and

2.2.4. In the bottom sequence of diagram (2.1)

$$M^*/N_{L/M}L^* \xrightarrow{N_{M/K}} K^*/N_{L/K}L^* \to K^*/N_{M/K}M^* \to 1,$$

the map $N_{M/K}$ is injective because the groups in this sequence have the respective orders $[L : M]$, $[L : K]$ and $[M : K]$ by Theorem 1.2.2. Therefore, $\hat{r}_{L/K}$ is an isomorphism.

Next, we show that $\hat{r}_{L/K} = r_{L/K}$ is an isomorphism for every finite abelian extension L/K. We prove this by induction on the degree. Write $G(L/K)$ as a direct sum of cyclic subgroups H_i and let M_i be the fixed field of H_i. One has $H_i = G(L/M_i)$ and M_i/K is an abelian subextension of L/K of smaller degree. For every M_i, consider $M = M_i$ in the diagram (2.1). The induction hypothesis says that $r_{M_i/K}$ is injective. Therefore, if $\sigma \in \ker(r_{L/K})$, then by the commutative diagram (2.1), one has σ is in the kernel of the map $G(L/K) \to G(M_i/K)$, which is equal to $G(L/M_i) = H_i$. In other words, the kernel of $r_{L/K}$ is contained in the intersection of those H_i. Since $G(L/K)$ is a direct sum of these H_i, the kernel of $r_{L/K}$ is the identity and hence $\hat{r}_{L/K}$ is injective. Surjectivity also follows by induction on the degree. Indeed, since $r_{M/K}$ and $r_{L/M}$ are surjective, so is $r_{L/K}$.

Finally, we note that $G(L/K)$ is solvable ([1, Chapter II]). If L/K is not abelian, then the commutator subgroup $G(L/K)'$ is neither the identity nor $G(L/K)$. Let M be the fixed field of $G(L/K)'$. One has M/K is an abelian extension and $G(L/M) = G(L/K)' \subsetneq G(L/K)$. Since $r_{M/K}$ is injective, the kernel of $r_{L/K}$ is contained in $G(L/M)$. Because $K^*/N_{L/K}L^*$ is abelian, $G(L/M) = G(L/K)'$ is also contained in the kernel of $r_{L/K}$, and hence $\ker(r_{L/K}) = G(L/M)$. This proves the injectivity of $\hat{r}_{L/K}$. The surjectivity follows by induction on the degree as in the abelian case. Indeed, since $[L : M] < [L : K]$, by the induction hypothesis, one has $r_{L/M}$ and $r_{M/K}$ are surjective, then so is $r_{L/K}$. Hence $\hat{r}_{L/K}$ is surjective. □

Putting L^{ab} the maximal abelian subextension of L/K, we find $G(L/K)^{\mathrm{ab}} = G(L^{\mathrm{ab}}/K)$. As an easy consequence of Theorem 2.2.7, we have the

Corollary 2.2.8. *Let L/K is a finite Galois extension and let L^{ab}/K be the maximal abelian subextension in L/K. Then $N_{L/K}L^* = N_{L^{\mathrm{ab}}/K}L^{\mathrm{ab}^*}$.*

3. The Existence Theorem

The reciprocity law gives us a very simple classification of the abelian extensions of a local field K. We first formulate the existence theorem by considering the norm topology. Then we use Lubin-Tate extension to show the existence theorem for the valuation topology.

3.1. The inverse of the mapping $\hat{r}_{L/K} : G(L/K)^{\mathrm{ab}} \to K^*/N_{L/K}L^*$ gives, for every finite Galois extension L/K a surjective homomorphism

$$(\quad, L/K) : K^* \to G(L/K)^{\mathrm{ab}}$$

with kernel $N_{L/K}L^*$. This map is called the *local norm residue symbol*. From Proposition 2.2.5, we have the

Proposition 3.1.1. *Let L/K and L_1/K_1 be finite Galois extensions such that K_1/K and L_1/L are finite separable extension. Then we have the commutative diagram*

$$\begin{array}{ccc} {K_1}^* & \xrightarrow{(\ ,L_1/K_1)} & G(L_1^{\mathrm{ab}}/K_1) \\ \downarrow{\scriptstyle N_{K_1/K}} & & \downarrow \\ K^* & \xrightarrow{(\ ,L/K)} & G(L^{\mathrm{ab}}/K) \end{array}$$

where the left vertical homomorphism are given by the norm map $N_{K_1/K}$ and the right vertical homomorphism is induced by the restriction $\sigma|_{L^{\mathrm{ab}}}$ of $\sigma \in G(L_1^{\mathrm{ab}}/K_1)$.

For every field K, we equip the group K^* with a topology by declaring the cosets $aN_{L/K}L^*$ to be a basis of neighborhoods of $a \in K^*$, where L/K varies over all finite Galois extensions of K. We call this topology the *norm topology* of K^*. Notice that by Corollary 2.2.8, we may just consider L/K varies over all finite abelian extensions of K. We will show latter that the norm topology is closely related to the valuation topology.

Lemma 3.1.2. *For every local field, we equip with the norm topology.*

1. *The open subgroups of K^* are precisely the closed subgroups of finite index.*
2. *The valuation $v_K : K^* \to \mathbb{Z}$ is continuous.*
3. *If L/K is a finite extension, then $N_{L/K} : L^* \to K^*$ is continuous.*

Proof.

(1) If $\mathcal{N}$ is a subgroup of K^*, then

$$\mathcal{N} = K^* \setminus \bigcup_{a\mathcal{N}\neq\mathcal{N}} a\mathcal{N}.$$

Now if $\mathcal{N}$ is open, then so are all cosets $a\mathcal{N}$, and hence $\mathcal{N}$ is closed. $\mathcal{N}$ is open also implies that one of the basis of open neighborhood of 1, $N_{L/K}L^*$ is contained in $\mathcal{N}$. From Theorem 2.2.7

$$\#(K^*/\mathcal{N}) \leq \#(K^*/N_{L/K}L^*) = \#G(L/K)^{\mathrm{ab}},$$

and hence $\mathcal{N}$ is also of finite index. If conversely $\mathcal{N}$ is closed and of finite index, then the union of the finitely many closed cosets $a\mathcal{N} \neq \mathcal{N}$ is closed, and so $\mathcal{N}$ is open.

(2) The groups $m\mathbb{Z}$, for $m \in \mathbb{N}$, form a basis of neighborhood of $0 \in \mathbb{Z}$, and if L/K is the unramified extension of degree m, then it follows that $v_K(N_{L/K}L^*) = mv_L(L^*) = m\mathbb{Z}$. This says that $N_{L/K}L^* \subseteq v_K^{-1}(m\mathbb{Z})$, which shows the continuity of v_K.

(3) Let $N_{M/K}M^*$ be an open neighborhood of 1 in K^*. Let F/L be a finite Galois extension which contains M. Then

$$N_{L/K}(N_{F/L}(F)^*) = N_{F/K}F^* \subseteq N_{M/K}M^*.$$

This says that $N_{F/L}F^* \subseteq N_{L/K}^{-1}(N_{M/K}M^*)$, which shows the continuity of $N_{L/K}$.

□

The finite abelian extensions L/K are now classified as follows.

Theorem 3.1.3. *Associating*

$$L \mapsto \mathcal{N}_L = N_{L/K}L^*$$

sets up a one-to-one correspondence between the finite abelian extensions L/K and the open subgroup $\mathcal{N}$ of K^* (equipped with the norm topology). Furthermore, this correspondence is an order reversing bijection and one has

$$\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} \quad \text{and} \quad \mathcal{N}_{L_1\cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}.$$

Proof. If L_1 and L_2 are finite abelian extensions of K, then the transitivity of the norm implies that $\mathcal{N}_{L_1L_2} \subseteq \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$. If conversely, $a \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, then from Proposition 3.1.1 $(a, L_1L_2/K)|_{L_1} = (a, L_1/K) = 1$ and $(a, L_1L_2/K)|_{L_2} = (a, L_2/K) = 1$. This implies that $(a, L_1L_2/K) \in G(L_1L_2/K)$ is the identity, and

hence $a \in \mathcal{N}_{L_1L_2}$. We therefore have $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, and so $\mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$ if and only if $\mathcal{N}_{L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} = \mathcal{N}_{L_1L_2}$ if and only if $[L_1L_2 : K] = [L_2 : K]$ (Theorem 2.2.7) if and only if $L_1 \subseteq L_2$. This also shows the injectivity of the correspondence $L \mapsto \mathcal{N}_L$.

If $\mathcal{N}$ is any open subgroup, then it contains $\mathcal{N}_{L_1}$ for some finite abelian extension L_1/K. But $(\mathcal{N}, L_1/K)$ is a subgroup of $G(L_1/K)$, so that $(\mathcal{N}, L_1/K) = G(L_1/L)$ for some subextension L/K. By the commutative diagram in Proposition 3.1.1, the kernel of $(\quad, L/K) : K^* \to G(L/K)$ is the full preimage of $G(L_1/L)$ under the map $(\quad, L_1/K) : K^* \to G(L_1/K)$, which is the group $\mathcal{N}$ since $(\mathcal{N}, L_1/K) = G(L_1/L)$, $\mathcal{N} \supseteq \mathcal{N}_{L_1}$ and $\mathcal{N}_{L_1}$ is the kernel of $(\quad, L_1/K)$. This implies that $\mathcal{N} = \mathcal{N}_L$ and shows that the correspondence is surjective.

Finally, the equality $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$ is obtained as follows. The order reversing property implies that $\mathcal{N}_{L_1 \cap L_2} \supseteq \mathcal{N}_{L_1}\mathcal{N}_{L_2}$. As $\mathcal{N}_{L_1}\mathcal{N}_{L_2}$ is open, the surjectivity of the correspondence implies that $\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \mathcal{N}_L$ for some finite abelian extension L/K. But $\mathcal{N}_{L_1} \subseteq \mathcal{N}_L$ and $\mathcal{N}_{L_2} \subseteq \mathcal{N}_L$ implies $L \subseteq L_1 \cap L_2$, so that $\mathcal{N}_{L_1 \cap L_2} \subseteq \mathcal{N}_L = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$. □

3.2. Formal groups are relevant for local class field theory in that they allow us to construct a perfect analogue of the theory of the p^n-th cyclotomic field extension over $\mathbb{Q}_p$, replacing $\mathbb{Q}_p$ by an arbitrary local field K. The formal groups provide an explicit version of the local reciprocity law.

Let $\widehat{K}$ be the completion of the maximal unramified extension $\widetilde{K}$ of K. We extend the Frobenius $\phi_K \in G(\widetilde{K}/K)$ to $\widehat{K}$ by continuity and denote it by ϕ. We remark that by the completeness, for $u \in U_K$, there exists $\varepsilon \in U_{\widehat{K}}$ such that $\varepsilon^{\phi-1} = u$, because the residue class field $\overline{k}$ of $\widehat{K}$ is algebraically closed. For a power series $F(x_1, \ldots, x_n) \in \mathcal{O}_{\widehat{K}}[[x_1, \ldots, x_n]]$, let $F^\phi(x_1, \ldots, x_n)$ be the power series in $\mathcal{O}_{\widehat{K}}[[x_1, \ldots, x_n]]$ by applying ϕ to the coefficients of $F(x_1, \ldots, x_n)$.

A (1-dimensional) *formal group* over $\mathcal{O}_K$ is a formal power series $F(x, y) \in \mathcal{O}_K[[x, y]]$ with the following properties:

(1) $F(x, y) \equiv x + y \pmod{\deg 2}$,
(2) $F(x, y) = F(y, x)$,
(3) $F(x, F(y, z)) = F(F(x, y), z)$.

From a formal group one gets an ordinary group by evaluating in a domain where the power series converge. If for instance $\overline{\mathfrak{P}}_K$ is the maximal ideal in the valuation ring of the algebraic closure $\overline{K}$ of K, then the operation $\alpha +_F \beta := F(\alpha, \beta)$ defines a new

structure of abelian group on $\overline{\mathfrak{P}}_K$. An endomorphism of the formal group $F(x,y)$ over $\mathcal{O}_K$ is a power series $f(x) \in \mathcal{O}_K[[x]]$ such that $F(f(x),f(y)) = f(F(x,y))$. The endomorphisms of $F(x,y)$ form a ring $\mathrm{End}_{\mathcal{O}_K}(F)$ in which addition and multiplication are defined by

$$(f +_F g)(x) = F(f(x),g(x)) \quad \text{and} \quad (f \circ g)(x) = f(g(x)).$$

Now, we introduce some properties of Lubin-Tate formal groups. We recommend the paper of Lubin and Tate [3] for the detail.

Let $k \simeq \mathbb{F}_q$ be the residue class field of K. A *Lubin-Tate* polynomial for a prime element π of K is by definition a polynomial $e(x) \in \mathcal{O}_K[x]$ of degree q with the properties

$$e(x) \equiv \pi x \pmod{\deg 2} \quad \text{and} \quad e(x) \equiv x^q \pmod{\mathfrak{P}_K}.$$

Lemma 3.2.1. *Let π and π' be prime element of K, and let $e(x), e'(x) \in \mathcal{O}_K[x]$ be Lubin-Tate polynomial for π and π', respectively. Let $L(x_1,\dots,x_n) = \sum_{i=1}^n a_i x_i$ be a linear form with coefficient $a_i \in \mathcal{O}_{\widehat{K}}$ such that*

$$\pi' L(x_1,\dots,x_n) = \pi L^{\phi}(x_1,\dots,x_n).$$

Then there is a uniquely determined power series $F(x_1,\dots,x_n) \in \mathcal{O}_{\widehat{K}}[[x_1,\dots,x_n]]$ satisfying

$$F(x_1,\dots,x_n) \equiv L(x_1,\dots,x_n) \pmod{\deg 2}$$

and

$$e'(F(x_1,\dots,x_n)) = F^{\phi}(e(x_1),\dots,e(x_n)).$$

Moreover, if the coefficients of $L(x_1,\dots,x_n)$ lie in $\mathcal{O}_K$, then $F(x_1,\dots,x_n)$ has coefficients in $\mathcal{O}_K$ as well.

Proof. It is immediately carried out putting $L_1(x_1,\dots,x_n) = L(x_1,\dots,x_n)$ and construct polynomials

$$L_{i+1}(x_1,\dots,x_n) \equiv L_i(x_1,\dots,x_n) \pmod{\deg i}$$

and

$$e'(L_{i+1}(x_1,\dots,x_n)) \equiv L_{i+1}^{\phi}(e(x_1),\dots,e(x_n)) \pmod{\deg i+1}.$$

Then $F(x_1,\dots,x_n) = \lim_{i\to\infty} L_i(x_1,\dots,x_n)$ is the desired series. □

Proposition 3.2.2. *Let π and π' be prime element of K, and let $e(x), e'(x) \in \mathcal{O}_K[x]$ be Lubin-Tate polynomial for π and π', respectively. Let $\pi' = u\pi$, $u \in U_K$,*

and $u = \varepsilon^{\phi-1}$, $\varepsilon \in U_{\widehat{K}}$. *Then there is a uniquely determined power series* $\theta(x) \in \mathcal{O}_{\widehat{K}}[[x]]$ *such that*

$$\theta(x) \equiv \varepsilon x \pmod{\deg 2} \quad \text{and} \quad e'(\theta(x)) = \theta^{\phi}(e(x)).$$

Furthermore, there is a uniquely determined power series $u(x) \in \mathcal{O}_K[[x]]$ *such that*

$$[u](x) \equiv ux \pmod{\deg 2} \quad \text{and} \quad e([u](x)) = [u](e(x)).$$

They satisfy

$$\theta^{\phi}(x) = \theta([u](x)).$$

Proof. Putting $L(x) = \varepsilon x$, we have $\pi' L(x) = \pi L^{\phi}(x)$ and the first claim follows immediately from Lemma 3.2.1. In the same way (with $\pi = \pi'$, $e(x) = e'(x)$ and the linear form $L(x) = ux$), one obtains the unique desired power series $[u](x) \in \mathcal{O}_K[[x]]$.

Finally, defining $\theta_1(x) = \theta^{\phi^{-1}}([u](x)$, we get $e'(\theta_1(x)) = \theta_1^{\phi}(e(x))$, and thus $\theta_1(x) = \theta(x)$ because the uniqueness. Hence $\theta^{\phi}(x) = \theta([u](x))$. □

Let $e(x) \in \mathcal{O}_K[x]$ be a Lubin-Tate polynomial for the prime element π, and let $F(x, y) \in \mathcal{O}[[x, y]]$ be the power series uniquely determined according to Lemma 3.2.1 (with $\pi = \pi'$, $e(x) = e'(x)$ and the linear form $L(x, y) = x + y$) such that

$$F(x, y) \equiv x + y \pmod{\deg 2} \quad \text{and} \quad e(F(x, y)) = F(e(x), e(y)).$$

Let $G(x, y) = F(y, x)$. Since $G(x, y)$ also satisfies the same condition $G(x, y) \equiv x+y \pmod{\deg 2}$ and $e(G(x, y)) = G(e(x), e(y))$, by the uniqueness of Lemma 3.2.1, one has $F(x, y) = F(y, x)$. In the same way, one obtains $F(x, F(y, z)) = F(F(x, y), z)$. This shows that $F(x, y)$ is a formal group. We call this formal group the *Lubin-Tate formal group* associated with $e(x)$.

For every $a \in \mathcal{O}_K$, we consider $L(x) = ax$ and again by Lemma 3.2.1, one obtain a unique $[a](x) \in \mathcal{O}_K[[x]]$ such that

$$[a](x) \equiv ax \pmod{\deg 2} \quad \text{and} \quad [a](e(x)) = e([a](x)).$$

Since $[a](F(x, y))$ and $F([a](x), [a](y))$ have the same linear term and both commute with $e(x)$, one obtains they are equal from the uniqueness of Lemma 3.2.1. This says that for every $a \in \mathcal{O}_K$, the power series $[a](x)$ is an endomorphism of $F(x, y)$ over $\mathcal{O}_K$. Follow the same pattern, by uniqueness, for every $a, b \in \mathcal{O}_K$ one has the following formulae.

(1) $[a + b](x) = F([a](x), [b](x))$,

(2) $[ab](x) = [a]([b](x))$,

(3) $[\pi](x) = e(x)$.

Hence, we have the

Proposition 3.2.3. *Let $F(x, y)$ be the Lubin-Tate formal group associated to a Lubin-Tate polynomial $e(x)$. For every $a \in \mathcal{O}_K$, the power series $[a](x) \in \mathcal{O}_K[[x]]$ is an endomorphism of $F(x, y)$ and it is an automorphism if and only if $a \in U_K$.*

Furthermore, the map $\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$ given by $a \mapsto [a](x)$ is a ring isomorphism.

Given the Lubin-Tate formal group $F(x, y)$ associated to a Lubin-Tate polynomial for π, we define the group of *π^n-torsion points* by

$$\Lambda_F(n) = \{\lambda \in \overline{\mathfrak{P}}_K \mid [\pi^n](\lambda) = [\pi]^{\circ n}(\lambda) = e^{\circ n}(\lambda) = 0\}.$$

For $a \in \mathcal{O}_K$, if $\lambda \in \Lambda_F(n)$ then

$$[\pi^n]([a](\lambda)) = [a\pi^n](\lambda) = [a]([\pi^n](\lambda)) = 0.$$

Hence, $\Lambda_F(n)$ is an $\mathcal{O}_K$-module and an $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module because it is killed by $\pi^n\mathcal{O}_K$.

Proposition 3.2.4. *$\Lambda_F(n)$ is a free $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module of rank 1.*

Proof. Since the highest term of $e^{\circ n}(x)$ is x^{q^n}, $\Lambda_F(n)$ consists of the q^n zeros of $e^{\circ n}(x)$ which is easily shown to be separable. Now if $\lambda \in \Lambda_F(n)\backslash\Lambda_F(n-1)$, then the mapping $\mathcal{O}_K \to \Lambda_F(n)$ defined by $a \mapsto [a](\lambda)$ is a homomorphism of $\mathcal{O}_K$-modules with kernel $\pi^n\mathcal{O}_K$. It induces an isomorphism $\mathcal{O}_K/\pi^n\mathcal{O}_K \to \Lambda_F(n)$ because both sides are of order q^n. □

Because $\Lambda_F(n) \simeq \mathcal{O}_K/\pi^n\mathcal{O}_K$ and $\mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_K/\pi^n\mathcal{O}_K) \simeq \mathcal{O}_K/\pi^n\mathcal{O}_K$, by taking the unit groups of these rings, we have the following.

Corollary 3.2.5. *Associating $a \mapsto [a](x)$ we obtain canonical isomorphism*

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(\Lambda_F(n)) \quad \text{and} \quad U_K/U_K^{(n)} \to \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_F(n)).$$

We now define the field of π^n-torsion points by

$$L_n = K(\Lambda_F(n)).$$

These fields are also called the *Lubin-Tate extensions*. L_n/K is the splitting field of the n-fold iteration $e^{\circ n}(x) = [\pi^n](x)$.

Theorem 3.2.6. *Let $F(x,y)$ be the Lubin-Tate formal group associated to a Lubin-Tate polynomial $e(x)$ for π. Then the field L_n/K of π^n-torsion points is a totally ramified abelian extension of degree $q^{n-1}(q-1)$ with Galois group*

$$G(L_n/K) \simeq \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_F(n)) \simeq U_K/U_K^{(n)}.$$

Furthermore, let $\lambda \in \Lambda_F(n) \setminus \Lambda_F(n-1)$. Then $L_n = K(\lambda)$ and $N_{L_n/K}(-\lambda) = \pi$.

Proof. If $e(x) = x^q + \pi(a_{q-1}x^{q-1} + \cdots + a_2x^2) + \pi x$, then

$$\begin{aligned} \Phi_n(x) &= \frac{e^{\circ n}(x)}{e^{\circ n-1}(x)} \\ &= (e^{\circ n-1}(x))^{q-1} + \pi(a_{q-1}(e^{\circ n-1}(x))^{q-2} + \cdots + a_2 e^{\circ n-1}(x)) + \pi \end{aligned}$$

is an Eisenstein polynomial of degree $q^{n-1}(q-1)$. If $\lambda \in \Lambda_F(n) \setminus \Lambda_F(n-1)$, then λ is clearly a zero of $\Phi_n(x)$, and is therefore a prime element of the totally ramified extension $K(\lambda)/K$.

Each $\sigma \in G(L_n/K)$ induces an automorphism of $\Lambda_F(n)$. We therefore obtain a homomorphism $G(L_n/K) \to \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_F(n))$. It is injective because L_n is generated by $\Lambda_F(n)$, and it is surjective because

$$\#G(L_n/K) \geq [K(\lambda) : K] = q^{n-1}(q-1) = \#(U_K/U_K^{(n)}).$$

□

We obtain the following explicit formula for the norm residue symbol of the Lubin-Tate extensions.

Theorem 3.2.7. *Let $F(x,y)$ be the Lubin-Tate formal group associated to a Lubin-Tate polynomial $e(x)$ for π. For the field L_n/K of π^n-torsion points and for $a = u\pi^m \in K^*$, $u \in U_K$, one has*

$$(a, L_n/K)\lambda = [u^{-1}](\lambda), \quad \lambda \in \Lambda_F(n).$$

Proof. Let $\sigma \in G(L_n/K)$ be the automorphism such that $\lambda^\sigma = [u^{-1}](\lambda)$, $\lambda \in \Lambda_F(n)$. We view σ as an element of $G(\widetilde{L}_n/K)$. Then $\tilde{\sigma} = \sigma\phi_{L_n}$ is an element of $\mathrm{Frob}(\widetilde{L}_n/K)$ such that $\sigma = \tilde{\sigma}|_{L_n}$ and $d_{L_n/K}(\tilde{\sigma}) = 1$ (because L_n/K is totally ramified). Let Σ be the fixed field of $\tilde{\sigma}$. Since $f_{\Sigma/K} = d_{L_n/K}(\tilde{\sigma}) = 1$, Σ/K is totally ramified. It has degree $q^{n-1}(q-1)$ because $\widetilde{\Sigma} = \widetilde{L}_n$.

Now let $\pi' = u\pi$ and let $F'(x,y) \in \mathcal{O}_K[[x,y]]$ be the Lubin-Tate formal group associated with a Lubin-Tate polynomial $e'(x)$ for π'. By Proposition 3.2.2, there exists a power series $\theta(x) = \varepsilon x + \cdots \in \mathcal{O}_{\widehat{K}}[[x]]$, with $\varepsilon \in U_{\widehat{K}}$, such that

$$\theta^\phi(x) = \theta([u](x)) \quad \text{and} \quad \theta^\phi(e(x)) = e'(\theta(x)), \quad (\phi|_{\widetilde{K}} = \phi_K).$$

Let $\lambda \in \Lambda_F(n) \setminus \Lambda_F(n-1)$ and consider $\pi_\Sigma = \theta(\lambda)$. Because

$$\pi_\Sigma^{\tilde{\sigma}} = \theta^\phi(\lambda^\sigma) = \theta^\phi([u^{-1}](\lambda)) = \theta(\lambda) = \pi_\Sigma,$$

(here we extend $\tilde{\sigma}$ to the completion $\widehat{L}_n$ of $\widetilde{L}_n$ by continuity), and λ is a prime element of L_n, one has π_Σ is a prime element of Σ. Since $e'^{\circ i}(\theta(\lambda)) = \theta^{\phi^i}(e^{\circ i}(\lambda))$, we have $\pi_\Sigma \in \Lambda_{F'}(n) \setminus \Lambda_{F'}(n-1)$. Hence $\Sigma = K(\pi_\Sigma)$ is the field of $(\pi')^n$-torsion points of $F'(x,y)$, and $N_{\Sigma/K}(-\pi_K) = \pi' = u\pi$ by Theorem 3.2.6. Since $\pi = N_{L_n/K}(-\lambda) \in N_{L_n/K}L_n^*$, we get

$$N_{\Sigma/K}(-\pi_\Sigma) \equiv u \pmod{N_{L_n/K}L_n^*} \quad \text{and} \quad a = u\pi^m \equiv u \pmod{N_{L_n/K}L_n^*},$$

and thus $r_{L_n/K}(\sigma) \equiv a \pmod{N_{L_n/K}L_n^*}$. This says that $(a, L_n/K) = \sigma$. □

Corollary 3.2.8. *Let $F(x,y)$ be the Lubin-Tate formal group associated to a Lubin-Tate polynomial $e(x)$ for π. The field L_n/K of π^n-torsion points is the class field relative to the group $(\pi) \times U_K^{(n)} \subseteq K^*$.*

Proof. For $a = u\pi^m$, we have $a \in N_{L_n/K}L_n^*$ if and only if $[u^{-1}](\lambda) = \lambda$ for all $\lambda \in \Lambda_F(n)$ if and only if $u^{-1} \in U_K^{(n)}$ if and only if $a \in (\pi) \times U_K^{(n)}$. □

3.3. Now we go back to the existence theorem. We claim that the subgroups of K^* which are open in the norm topology are precisely the subgroups of finite index which are open in the valuation topology.

A subgroup $\mathcal{N}$ which is open in the norm topology by Theorem 3.1.3 is a group of norms $N_{L/K}L^*$ of a finite abelian extension L/K. By Theorem 2.2.7, $\mathcal{N}$ is of finite index in K^*. In order to show that $N = N_{L/K}L^*$ is open in the valuation topology, we need to show that $N_{L/K} : L^* \to K^*$ is a continuous map with respect to the valuation topology. This is true because $U_K^{(n)}$ is an open neighborhood of 1 and there exists a large enough m such that $N_{L/K}U_L^{(m)} \subseteq U_K^{(n)}$.

Proposition 3.3.1. *Suppose that $\mathcal{N}$ is a subgroup of K^*. Then $\mathcal{N}$ is open in the norm topology if and only if $\mathcal{N}$ is of finite index in K^* and is open in the valuation topology.*

Proof. Suppose that $\mathcal{N}$ is open in the norm topology. Then $\mathcal{N}$ is a group of norms $N_{L/K}L^*$ of a finite abelian extension L/K, and hence has finite index in K^*. $\mathcal{N}$ is also open in the valuation topology because it contains the subgroup $N_{L/K}U_L$ which itself is open in the valuation topology. In fact, because $N_{L/K} : L^* \to K^*$

is continuous in the valuation topology, $N_{L/K}U_L$ being the image of the compact group U_L is closed and of finite index in U_K, and hence it is open.

For the converse, it suffices to verify that a subgroup $\mathcal{N}$ of finite index in K^* which is open in the valuation topology contains the norm subgroup $N_{L/K}L^*$ of some finite Galois extension L/K. Let π_K be a prime element of K. Since $\mathcal{N}$ is of finite index in K^*, there exists $f \in \mathbb{N}$ such that $\pi_K^f \in \mathcal{N}$. Moreover, since $\mathcal{N}$ is open and $U_K^{(i)}$, $i \in \mathbb{N}$ is a basis of open neighborhood of 1, there exists $n \in \mathbb{N}$ such that $U_K^{(n)} \subseteq \mathcal{N}$. Therefore, the group $(\pi_K^f) \times U_K^{(n)}$ is contained in $\mathcal{N}$. The class field of $(\pi_K^f) \times U_K$ is the unramified extension K_f/K of degree f, because $N_{K_f/K}(\pi_K) = \pi_K^f$ and $N_{K_f/K}(U_{K_f}) = U_K$. By Corollary 3.2.8, the class field of $(\pi_K) \times U_K^{(n)}$ is the field L_n/K of π_K^n-torsion points. Therefore, by Theorem 3.1.3 the class field of the group

$$(\pi_K^f) \times U_K^{(n)} = ((\pi_K^f) \times U_K) \cap ((\pi_K) \times U_K^{(n)})$$

is $K_f L_n = L$, and hence $N_{L/K}L^* \subseteq \mathcal{N}$. □

Now, we know that the subgroups of K^* which are open in the norm topology are precisely the subgroups of finite index which are open in the valuation topology. Hence we obtain the existence theorem.

Theorem 3.3.2 (Existence Theorem)**.** *Associating $L \mapsto \mathcal{N}_L = N_{L/K}L^*$ sets up a one-to-one correspondence between the finite abelian extensions L/K and the open subgroup $\mathcal{N}$ of finite index in K^* (with respected to the valuation topology).*

The existence theorem gives the *local Kronecker-Weber Theorem*:

Theorem 3.3.3. *Every finite abelian extension of $L/\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$, where ζ is a root of unity.*

Proof. Since L/K is finite, for suitable f, we have $p^f \in N_{L/K}L^*$. Because $N_{L/\mathbb{Q}}L^*$ is open (Theorem 3.3.2), we have $U_{\mathbb{Q}_p}^{(n)} \subseteq N_{L/\mathbb{Q}_p}L^*$, for n sufficiently large.

The class field for $(p^f) \times U_{\mathbb{Q}_p}$ is the unramified extension $\mathbb{Q}_p(\zeta_1)/\mathbb{Q}_p$ of degree f, where ζ_1 is a primitive $(p^f - 1)$-th root of 1. Consider the Lubin-Tate polynomial $e(x) = (1 + x)^p - 1$. Let ζ_2 be a primitive p^n-th root of 1. Then $\zeta_2 - 1$ is the primitive element for the p^n-torsion points of the Lubin-Tate formal group.

Therefore L is contained in the class field M of

$$(p^f) \times U_{\mathbb{Q}_p}^{(n)} = ((p^f) \times U_{\mathbb{Q}_p}) \cap ((p) \times U_{\mathbb{Q}_p}^{(n)}).$$

By Theorem 3.1.3, M is the composite of $\mathbb{Q}_p(\zeta_1)$ and $\mathbb{Q}_p(\zeta_2)$. M is therefore equal to $\mathbb{Q}_p(\zeta)$ where ζ is a primitive $(p^f-1)p^n$-th root of 1. □

References

[1] I. B. Fesenko & S. V. Vostokov, Local Field and Their Extensions (A Constructive Approach), *Translations of Mathematical Monographs* **121**, American Mathematical Society, Providence, 1993.

[2] S. Lang, *Algebra*, Addison-Welsley, Menlo Park, 1984.

[3] J. Lubin & J. Tate, *Formal Complex Multiplication in Local Field*, Ann. Math. 81 (1965) pp. 380–387.

[4] J. Neukirch, Class Field Theory, *Grundlehren der mathematischen Wissenschaften* **280**, Springer-Verlag, Berlin Heidelberg, 1986.

[5] J.-P. Serre, Local Fields, *Graduate Texts in Mathematics* **67**, Springer-Verlag, New York, 1995.

Department of Mathematics, National Taiwan Normal University
E-mail address: li@math.ntnu.edu.tw