Chin. Ann. of Math.
10B (2) 1989

FORMAL GROUPS AND LOCAL CLASS FIELD THEORY*

Li Delang (李德琅)**

Abstract

The purpose of this paper is to prove that every abelian extenison of a local field can be embedded into certain generalized Lubin-Tate extensions. As a consequence of the embedding theorem, a new proof of local class field theory is given, which looks more intuitive than Galois cohomology. Also the author gets a necessary and sufficient condition for a totally ramified extension of degree p to be normal in terms of the coefficients of its definition equation.

§1. Introduction

Suppose K is a local field. To study abelian extensions of K, Lubin and Ta
defined a special kind of abelian extensions of K by using formal group theory o
as Lubin and Tate called it, formal complex multiplication, Hazewinkel gave a ne
proof of local class field theory without Galois cohomology.

In the present paper we prove that every totally ramified abelian extension
local field K can be embedded into Lubin-Tate extensions $L_{\pi,m}$ for certain m if an
only if π lies in the norm from L. Furthermore every abelian extension of K ca
be embedded into certain generalized Lubin-Tate extension. Henceforth we ca
define reciprocity map and calculate the kernel. We get local class field theory in
way different from [2]. More precisely we do not use an "almost reciprocity ma
based on the snake lemma as used in [2] but we use more formal groups. Also v
get a necessary and sufficient condition for a totally wildly ramified extension
degree p, the characteristic of the residue field, to be normal, which makes it possib
to distinguish a normal Eisenstein polynomial of degree p by its coefficients.

The embedding theorem for tamely ramified extensions follows fro
Krasners's lemma. To deal with the wildly totally ramified case we begin wi
extension of degree p. We find first a necessary condition for such extension to
normal, then we compute the number of extensions satisfying this condition und

Manuscript received October 13, 1986. Revised April 1, 1987,

* The Project Supported by National Natural Science Foundation of China

** Department of Mathematics, Sichuan University, Chengdu, Sichuan, China.

ome restrictions and of the subextensions of $L_{\pi,m}/K$ for certain m and we see that hese two numbers are equal. Hence this condition is also sufficient and every xtension verifying this condition can be embedded into $L_{\pi,m}$. Finally we get the ;eneral embedding theorem from this special case with the help of Galois theory.

§2. Preliminary and Notations

In this section we collect the notations and the results that will be used in the ollowing. The proofs can be found in the standard texts, for example [4, 5] (for ›cal fields) and [1] (for formal groups).

.1 Notations for local fields

By a local field we mean a field K with a normalized exponential valuation $_K$: $K^*\to\mathbb{Z}$ on it such that K is complete and the residue field is finite. We define

$$A(K)=\{x\in K\mid v_K(x)\geqslant 0\},\ \text{the ring of integers of } K,$$

$$U(K)=\{x\in K\mid v_K(x)=0\},\ \text{the group of the units of } K,$$

π_K, a uniformizing element of K,

$$\mathscr{M}(K)=\{x\in K\mid v_K(x)>0\},\ \text{the maximal ideal of } A(K),$$

$$U_m(K)=\{x\in U(K)\mid x\equiv 1\ (\text{mod } \mathscr{M}_K^m)\},$$

$$\overline{K}=A(K)/\mathscr{M}(K),$$

ıe residue field of K, which is always assumed to be finite.

$$K^*=K\backslash 0,\ \text{the invertible elements of } K.$$

.2 Formal groups and Lubin-Tate extension

Let K be a local field and E/K an unramified extension. Let σ be the Frobenius ıbstitution.

Let
$$g(X)=X+\sum_{i=1}^{\infty}b_ix^i$$
ə a power series over $A(E)$, and $f(X)$ be a power series over E satisfying

$$f(X)-\pi^{-1}\sigma_*f(X^q)=g(X),$$

here $\pi=\pi_K$ and σ_* denotes the substitution obtained by acting σ on the coefficients f f. We call

$$F(X,Y)=f^{-1}(f(X)+f(Y))$$

twisted Lubin -Tate formal group associated to π. When $E=K$, we simply call '(X, Y) a Lubin-Tote formal group associated to π.

We have a homomorphism of rings from $A(K)$ to the endomorphism ring of F hich sends $a\in A(K)$ to the power series $[a]_f=f^{-1}(af(X))$. It is known that

$$[\pi]_f\equiv X^q+\pi X\quad(\text{mod } \pi,\ \text{degree } 2)$$

and there are elements $\lambda_n\in\Omega$ such that

$$[\pi]_f(\lambda_1)=0,$$

$$[\pi]_f(\lambda_n)=\lambda_{n-1}.$$

Let $L_{\pi,m}=K(\lambda_m)$. Then $L_{\pi,m}$ is a totally ramified extension of degree $q^{m-1}(q-1)$ of K and is called the m–th Lubin–Tate extension associated to π.

There exists a homomorphism ρ from the group of units $U(K)$ onto the Galois group Gal $(L_{\pi,m}/K)$ such that

$$\rho(u)(\lambda_m)=[u]_f(\lambda_m)$$

with kernel

$$\ker\rho=U_m(K)=\mathrm{N\ orm}_{L_{\pi,m}/K}(U_{L_{\pi,m}}).$$

Let $G(X, Y)$ be a twisted Lubin–Tate formal group associated to π defin over an unramified extension K/K with logarithm g. Then the roots of the equati

$$[\pi]_g(X)=0$$

define a totally ramified extension $L_{\pi,m}(E)$ over E. We have

$$f^{-1}(g(X))\in A(E)[\![X]\!].$$

Suppose that μ is a root of $[\pi]_g(X)=0$. Then $f^{-1}(g(\mu))$ is a root of the equati $[\pi]_f(X)=0$. Therefore $L_{\pi,1}\cdot E\subset L_{\pi,1}(E)$. Similarly we get the opposite inclusi and henceforth $L_{\pi,1}E=L_{\pi,1}(E)$. We call $L_{\pi,1}(E)$ a generalized Lubin–Tate extensi of K with respect to E and π. Similarly we define m–th generalized Lubin–Ta extension of K with respect to E and π.

For the proof see [3] or [1].

§ 3. Reciprocity Map

In this section, we define the reciprocity map for any subextension of generalized Lubin–Tate extension and prove that it is well–defined, that is, it . independent of the Lubin–Tate extension used in the definition. We leave th calculation of its kernel to the next sections.

Let π and π_1 be uniformizing elements of K. Let $L_{\pi,m}$ and $L_{\pi 1,m}$ be the Lubin Tate extensions associated to π and π_1 respectively. Suppose that E/K is an un ramified extension.

Theorem 1. *If there exists an element $b\in U(K)$ such that*

$$v(\pi b/\pi_1\sigma b-1)\geqslant m,$$

where σ is the Frobenius substitution, then we have $L_{\pi,m}(E)=L_{\pi_1,m}(E)$.

Proof Let F (resp. F_1) be a Lubin–Tate formal group associated to π (resp. π_1 and f (resp. f_1), the logarithm of F (resp. F_1). Then one has

$$f-\pi\sigma_* f(X^q)=g(X)\in A(K)[\![X]\!].$$

Multiplying this equation by b one gets

$$bf-(b\pi/\sigma b)\sigma_* bf(X^q)=bg(X)\in A(E)[\![X]\!].$$

Let $\pi_2=b\pi/\sigma b$ and let $F_2(X, Y)$ be the twisted Lubin–Tate formal group defined

$A(E)$ associated to π_2 and f_2 the logarithm of $F_2(X, Y)$. By Hazewinkel lemma ${}^1(f_2(X))$ is in $A(E)[[X]]$ and is an isomomorphism from F_2 to F. Therefore

$$L_{\pi,m}(E)=L_{\pi_2,m}(E).$$

t

$$[\pi_1]_{f_1}(X)=\Sigma a_iX^i,$$
$$[\pi_2]_{f_2}(X)=\Sigma b_iX^i.$$

e may assume by Lubin-Tate lemma that

$$a_1\equiv b_1 \pmod{\pi^{m+1}},\ a_i=b_i,\ i\geqslant 2$$

ıce by the assumption

$$\pi_1\equiv\pi_2 \pmod{\pi^{m+1}}.$$

Let $p_1(X)=[\pi_1]_{f1}(X)/X$, $p_2(X)=[\pi_2]_{f_2}(X)/X$. Let α_1 (resp. β_1) be a root of (X) (resp. $p_2(X)$)). Then

$$L_{\pi,1}(E)=E(\alpha_1)^*$$
$$L_{\pi_2,1}(E)=E(\beta_1).$$

ıe has

$$p_2(\alpha_1)\equiv 0 \pmod{\pi^{m+1}},$$
$$p_2'(\alpha_1)\equiv(q-1)\alpha^{(q-2)} \pmod{\pi^{m+1}}.$$

ɾ Newton method there exists an element $\alpha\in L_{\pi_2,1}(E)$ such that

$$p(\alpha)=0,$$
$$\alpha-\lambda_1'\equiv0 \pmod{\pi^m\lambda_1'}.$$

ence one gets

$$L_{\pi,1}(E)=L_{\pi_2,1}(E)$$

ıd can assume that

$$\lambda_1-\lambda_1'\equiv0 \pmod{\pi^m\lambda_1}.$$

The equations

$$[\pi]_F(X)=\lambda_1$$
$$[\pi_2]_{F_2}(X)=\lambda_1'$$

fine $L_{\pi,2}(E)$ and $L_{\pi_2,2}(E)$ respectively. One has

$$[\pi_2]_{F_2}((\lambda_2)\equiv\lambda_1'-\lambda_1 \pmod{\pi^{m+1}},$$

.d therefore

$$[\pi_2]_{F_2}(\lambda_2)\equiv0 \pmod{\pi^m\lambda}.$$

ı the other hand

$$\frac{d}{dx}[\pi_2]_{F_2}(\lambda_2)\equiv\pi_2 \pmod{\pi^2}.$$

, if $m\geqslant2$, we can use Newton method again and obtain $\beta\in L_{\pi,2}(E)$ such that

$$[\pi_2]_{F_2}(\beta)=\lambda_1'^*$$
$$\beta-\lambda_2'\equiv0 \pmod{\pi^{m-1}\lambda_1}.$$

This shows that $L_{\pi,2}(E)=L_{\pi_2,2}(E)$ and we may assume that $\beta=\lambda_2'$ and

$$\lambda_2-\lambda_2'\equiv0 \pmod{\pi^{m-1}\lambda_1}.$$

Continuing this trick one gets

$$L_{\pi,i}(E)=L_{\pi_1,i}(E),$$
$$\lambda_i-\lambda_i'\equiv 0 \pmod{\pi^{m-i+1}\lambda_1}$$

for all $i\leqslant m$.

Remark. The inverse of the theorem is also true, but we do not need it.

Theorem 2. *Let π and π_1 be uniformizing elements of $A(K)$. Let m be a positive integer. Then there exists an unramified extension E/K (depending on π, π_1 and m) such that*

$$L_{\pi,m}(E)=L_{\pi_1,m}(E).$$

Proof It is enough to find out an unramified extension E and $b\in A(E)$ suc that $v(\pi_1-\pi b/\sigma b)\geqslant m+1$, where σ is the Frobenius substitution. So the theore follows from induction and the following Lemma.

Lemma 1. *Let c be an element of $U(K)$ such that $c\equiv 1 \pmod{\pi^n}$, $n\geqslant 0$. The there exists an unramified extension E/K and $b\in A(E)$ such that*

$$c\equiv\sigma b/b \pmod{\pi^{n+1}}$$

and

$$b\equiv 1 \pmod{\pi^n}.$$

Proof First suppose $n=0$. Let b be a root of the equation

$$X^{q-1}=c.$$

Then $K(b)=E$ is an unramified extension of K and

$$\sigma b\equiv b^q\equiv bc \pmod{\pi}.$$

Suppose now $n\geqslant 1$ and

$$c\equiv 1+d\pi^n \pmod{\pi^{n+1}}.$$

Consider the equation

$$h(X)=X^q-X-d=0.$$

Any root a of $h(X)=0$ defines an unramified extension since

$$h'(X)=qX^{q-1}-1\equiv -1 \pmod{\pi}.$$

One has

$$\sigma a\equiv a^q\equiv a+d \pmod{\pi}.$$

Let

$$b=1+a\pi^n.$$

Then

$$\sigma b=1+\pi^n\sigma a\equiv 1+(a+d)\pi^n\equiv(1+a\pi^n)(1+d\pi^n)\equiv bc \pmod{\pi^{n+1}}.$$

Let Σ be the maximal unramified extension of K. It is not complete. Let Σ_1 t its completion.

Theorem 3. *Let F and F_1 be Lubin-Tate formal groups associated to π and respectively. Then F and F_1 are isomorphic over the integer ring $A(\Sigma_1)$ of the field Σ*

Proof Let $c=\pi_1/\pi\in U(K)$. Then by Lemma 1 there exist $b_i\in\Sigma$ such that

$$c\prod_{i=1}^{m}b_i/\sigma\prod_{i=1}^{m}b_i\equiv 1 \pmod{\pi^{m+1}},$$

$$b_i \equiv 1 \pmod{\pi^m}.$$

The sequence $\left\{\prod_{i=1}^{m} b_i\right\}$ is a Cauchy sequence. Hence there exists a $b \in \Sigma_1$ such that

$$b = \lim_{m\to\infty} \prod_{i=1}^{m} b_i.$$

Therefore

$$cb/\sigma b = 1.$$

Let f and f_1 be the logarithm of F and F_1 respectively. Then

$$f(X) - \pi^{-1}\sigma_* f(X^q) = g(X) \in A(K)[\![X]\!],$$
$$f_1(X) - \pi_1^{-1}\sigma_* f_1(X^q) = g_1(X) \in A(K)[\![X]\!].$$

Hence

$$bf(X) - \frac{b\pi^{-1}}{\sigma b}\,\sigma_* bf(X^q) = bg(X) \in A(\Sigma_1)[\![X]\!],$$

i. e.,

$$bf(X) - \pi_1^{-1}\sigma_* b\, f(X^q) = bg(X).$$

It follows from Hazewinkel lemma that

$$f_1^{-1}(bf(X)) \in A(\Sigma_1)[\![X]\!].$$

Let $L_{\pi,m}$ be a Lubin-Tate extension of K. We can define the reciprocity map

$$R_m\colon K^* \to \mathrm{Gal}(L_{\pi,m}\Sigma/K)$$

as follows:

$$R_m(u)\,|_{L_{x,m}} = \rho(u^{-1}),\ R_m(u)\,|_{\Sigma} = \mathrm{id.}\ \text{for}\ u \in U(K),$$
$$R_m(\pi)\,|_{L_{x,m}} = \mathrm{id.},\ R_m(\pi)\,|_{\Sigma} = \sigma,$$

where σ is the Frobenius automorphism.

By Theorem 3, $L_{\pi,m}\Sigma = L_{\pi_1,m}\Sigma$ for any uniformizing elements π and π_1 of K.

Theorem 4. *The reciprocity map is independent of the choice of π.*

Proof Let π be anotner uniformizing element of K. Define

$$R'_m\colon K^* \to \mathrm{Gal}(L_{\pi_1,m}\Sigma/K) = \mathrm{Gal}(L_{\pi,m}\Sigma/K)$$

by

$$R'_m(u)\,|_{L_{\pi_1,m}} = \rho_1(u^{-1}),\ R'_m(u)\,|_{\Sigma} = \mathrm{id.}\ \text{for}\ u \in U(K),$$
$$R'_m(\pi_1)\,|_{L_{\pi_1,m}} = \mathrm{id.},\quad R'_m(\pi_1)\,|_{\Sigma} = \sigma,$$

where $\rho_1(u^{-1})$ is defined by

$$\rho_1(u^{-1})(\lambda'_m) = f_1^{-1}(u^{-1} f_1(\lambda'_m)).$$

We have to show that $R_m = R'_m$.

Let $\pi_1 = \pi c_1 c \in U(K)$. Then by Theorem 3 there exists a unit b in Σ_1 such that $= (\sigma b)/b$ and $f_1^{-1}(bf(X))$ is an isomorphism from F to F_1 over Σ_1. We may assume hat $\lambda'_m = f_1^{-1}(bf(\lambda_m))$ since the right hand side is a root of the equation

$$[\pi_1^m]_F(X)/[\pi_1^{m-1}]_{F1}(X) = 0.$$

We can view $R(a)$ and $R_1(a)$, $a \in K^*$, as an automorphism of $L_{x,m}\Sigma_1 = L_{\pi_1,m}\Sigma_1$ keeping K fixed. Then for $u \in U(K)$ we have

$$\begin{aligned} R(u)(\lambda'_m) &= R(u) f_1^{-1}(bf(\lambda_m)) \\ &= f_1^{-1}(bf(R(u)(\lambda_m))) \\ &= f_1^{-1}(bf(f^{-1}(uf(\lambda_m)))) \\ &= f_1^{-1}(buf(\lambda_m)) = f_1^{-1}(uf_1(f_1^{-1}(uf(\lambda_m)))) \\ &= f_1^{-1}(uf_1(\lambda'_m)) = R_1(u)(\lambda'_m), \end{aligned}$$

which implies $R(u)=R_1(u)$. Furthermore

$$\begin{aligned} R(\pi_1)(\lambda'_m)) &= R(\pi)\cdot R(c)(\lambda'_m) \\ &= R(\pi)\cdot R(c)(f_1^{-1}(bf(\lambda_m)) \\ &= R(\pi) f_1^{-1}(bf(f^{-1}(cf(\lambda_m)))) \\ &= R(\pi) f^{-1}(bcf(\lambda_m)) \\ &= f_1^{-1}((\sigma b)cf(\lambda_m)) = f_1^{-1}(bf(\lambda_m)) = \lambda'_m. \end{aligned}$$

Hence

$$R_m(\pi_1)\,|_{L_{\pi 1,m}} = \mathrm{id}.$$

On the other hand

$$R_m(\pi_1)\,|_\Sigma = R_m(\pi) R_m(c)\,|_\Sigma = \sigma.$$

Therefore

$$R_m(\pi_1) = R'_m(\pi_1).$$

Now suppose L/K is a finite subextension of $L_{\pi,m}\ \Sigma/K$. We can define tl reciprocity map

$$R_L\colon K^* \to \mathrm{Gal}(L/K)$$

by restriction:

$$K^* \xrightarrow{R_m} \mathrm{Gal}\,(L_{\pi,m}\Sigma/K) \xrightarrow{\text{res.}} \mathrm{Gal}(L/K).$$

It is independent of the choice of π and m by Theorem 4 and the fact that

$$\lambda_m = [\pi^i]_F(\lambda_{m+i})$$

and

$$[u]_F(\lambda_m) = [\pi^i]_F([u]_F(\lambda_{m+i})).$$

§ 4. Kernel of the Reciprocity Map (Totally Ramified Case)

Let $L_{\pi,m}$ be a Lubin-Tate extension. We already know that the kernel reciprocity map is

$$U_m\cdot\langle\pi\rangle = \mathrm{Norm}\ _{L_{\pi,m}}/K\,(L^*_{\pi,m}).$$

We want to find out the kernel of reciprocity map R_L for totally ramified extensic L/K.

Definition. *Let L/K be a totally ramified abelian extension. We say L/K h the embedding property if for any $\pi\in N_{L/K}(L^*)$, where π is a uniformizing eleme of K, there exists a positive integer m such that $L\subset L_{\pi,m}$.*

Theorem 5. *If L/K is a totally ramified abelian extension having the embedding* *property, then* ker $R_L = N_{L/K}(L^*)$.

Proof Let π be a uniformizing element of K such that $\pi \in N_{L/K}(L^*)$. Then $\pi \in \ker R_L$ since $\pi \in \ker R_{L_{\pi,m}}$ and $R_L(\pi) = R_{L_{\pi,m}}(\pi)\,|_L$. Let a be an element of K lying in $N_{L/K}(L^*)$. Then there exists an integer n such that $a\ \pi^{-n} \in N_{L/K}(L^*)$ and $a\ \pi^{-n}$ is a uniformizing element of K. Therefore $a\ \pi^{-n} \in \ker R_L$, which implies $a \in \ker R_L$. This shows

$$N_{L/K}(L^*) \subset \ker R_L.$$

Suppose π_1 is a uniformizing element of K lying outside of $N_{L/K}(L^*)$. Then clearly $L \not\subset L_{\pi_1, m}$. By Theorem 2 there exists an unramified extension E/K such that

$$L_{\pi, m}E = L_{\pi_1, m}E;$$

we call this field M. It is clear that $L \subset M$ since $L \subset L_{\pi, m}$. We have

$$R_M\,|_L = R_L.$$

Let H be the subgroup of Gal (M/K) generated by $R_M(\pi_1)$. The fixed field of H is $L_{\pi_1, m}$ since it contains $L_{\pi_1, m}$ and has the same degree. This means

$$R_L(\pi_1) = R_M(\pi_1)\,|_L \neq \text{id}.$$

since $L \not\subset L_{\pi_1, m}$.

§ 5. Embedding Theorems I

In this section we prove that every cyclic totally ramified abelian extension L/K of degree p or of degree d, $(d, p) = 1$, has the embedding property.

Proposition 1. *Let L/K be a totally tamely ramified cyclic extension of degree d, $(d, p) = 1$. Then $L \subset L_{\pi, 1}$ for any uniformizing element $\pi \in N_{L/K}(L^*)$ and $d\,|\,(q-1)$.*

Proof Let $\alpha \in L$ be a uniformizing element of L such that $N_{L/K}(\alpha) = \pi$. Then α satisfies an Eisenstein equation

$$h(X) = X^d + a_1X^{d-1} + \cdots + a_d = 0,$$

where $a_i \in (\pi)$ and $a_d = (-1)^d\pi$. The different $D(L/K)$ is (α^{d-1}) since

$$r'(\alpha) \equiv \alpha^{d-1} \pmod{\mathscr{M}}.$$

Then

$$v(\tau\alpha - \alpha) = 1/d \text{ for any } \tau \in \mathrm{Gal}(L/K) = G$$

since $v(\tau\alpha - \alpha) \geqslant 1/d$ and

$$v(\prod_{\tau \in G, \tau \neq 1} (\tau\alpha - \alpha)) = v(h'(\alpha)) = (d-1)/d.$$

Hence

$$\tau\alpha \equiv u\alpha \pmod{\alpha^2}$$

for some $u \in U(K) \setminus U_1(K)$.

The mapping

$$\phi\colon G \to U(K)/U_1(K)$$
$$\tau \to \tau\alpha/\alpha \cdot U_1(K)$$

is a group homomorphism and is injective for otherwise we have $\tau\alpha/\alpha\in U_1(K)$ for $\tau\neq 1$, a contradiction. This implies $d=|G|$ is a divisor of

$$(q-1)=|U(K)/U_1(K)|.$$

Therefore one can find an element $\beta\in\mathcal{A}(L_{\pi,1})$ with $v(\beta)=1/d$. Using $\omega\beta$ instead of β for some $\omega\in U(K)$ if necessary we may assume $v(\beta-\alpha)>1/d$. This means

$$u(\beta-\alpha)>v(\tau\alpha-\alpha) \text{ for all } \tau\in G.$$

Applying Krasner Lemma[5] one sees

$$K(\alpha)\subset K(\beta)\subset L_{\pi,1}.$$

To study wild ramification we start from the simplest case of a cyclic extensi of degree p. The idea is counting the nnmber of such extensions by making use Krasner lemma and different and comparing it with the number of subextensi of $L_{\pi,m}/K$ of degree p.

Let L/K be a totally ramified cyclic extension of degree p. Let $L=K(\alpha)$, wh α is a uniformizing element of L satisfying the Eisenstein equation

$$h(X)=X^p+a_1X^{p-1}+\cdots+a_{p-1}X+a_p=0$$

where $a_i\in\mathcal{M}(K)$ and

$$a_p=(-1)^p\pi=(-1)^pN_{L/K}(\alpha).$$

The different $D(L/K)$ is generated hy $h'(\alpha)$ and

$$v(h'(\alpha))=\min\{v(p\alpha^{p-1}),\ v(a_i\alpha^{p-i-1}),\ i=1,\ \cdots,\ p-1\}.$$

Suppose $G=\mathrm{Gal}(L/K)$ and G_t is the last non-trivial ramification group. Then $\tau\in G$ and $\tau\neq id.$, we have

$$v(\alpha-\tau\alpha)=v(\alpha^{t+1})=\frac{t+1}{p}.$$

Let $k=[v(h'(\alpha)]$, the largest integer less than or equal to $v(h'(\alpha))$. Let $r=t-k$.

If $v(h'(\alpha))=v(a_j\alpha^{p-j-1})$, then $k=v(a_j)$ and $K=(p-1)r+j$ since

$$k+\frac{p-j-1}{p}=v(h'(\alpha))=\prod_{\tau\neq 1}v(\alpha-\tau\alpha)=\frac{(p-1)(t+1)}{p}.$$

In this case one sees

$$\begin{aligned}&v(a_i)\geqslant k \quad \text{for } i\leqslant j;\\ &v(a_i)>k \quad \text{for } j<i\leqslant p-1;\\ &v(p)>k.\end{aligned}$$

If $v(h'(\alpha))=v(p\alpha^{p-1})=v(p)+(p-1)/p$, then

$$\begin{aligned}&v(a_i)>k \text{ for } 1\leqslant i\leqslant p-1,\\ &v(p)=k=(p-1)r.\end{aligned}$$

Lemma 2. *Let L/K be as above and define t, k, r, j as above.*

If $\beta\in\Omega$ is a root of the equation

$$X^p+b_1X^{p-1}+\cdots+b_{p-1}X+b_p=0,$$

where $b_p=(-1)^p\pi=a_p$ and

$$a_i\equiv b_i \pmod{\pi^{k+r+1}} \text{ for } i=1,\ \cdots,\ p-1,$$

hen $K(\alpha)=K(\beta)$.

Proof One has

$$h(\beta)=\sum_{i=1}^{\beta-1}(a_i-b_i)\beta^{p-i}\equiv 0 \pmod{\pi^{k+r+1}\beta}.$$

ince

$$h(\beta)=\prod_{\tau\in G}(\beta-\tau\alpha),$$

here exists a $\tau\in G$ such that

$$v(\beta-\tau\alpha)\geqslant v(\pi^{k+r+1}\beta)/p>(k+r+1)/p=(t+1)/p=v(\alpha-\tau\alpha).$$

Ience $\alpha\in K(\beta)$ by Krasner lemma. But $K(\alpha)$ and $K(\beta)$ are extensions of the same legree, they must be equal.

Lemma 3. 1) *If $k<v(p)$, there exist at most $q^{k-1}(q-1)/(p-1)$ cyclic totally amified extensions L/K of degree p such that $\pi\in N_{L/K}(L^*)$ and*

$$k\leqslant v(D(L/K))<k+(p-1)/p.$$

2) *If $k=v(p)\equiv 0 \pmod{p-1}$, there is no cyclic totally ramified extension L/K f degree p with*

$$k\leqslant v(D(L/K))<k+1.$$

f $k=v(p)\equiv 0 \pmod{p-1}$ and $p\not\equiv u^{p-1}\pi^k \pmod{\pi^{k+1}}$ for any $u\in U(K)$, there is no uch extension; if $k=v(p)\equiv 0 \pmod{p-1}$ and $p\equiv u^{p-1}\pi^k \pmod{\pi^{k+1}}$ for certain $\in U(K)$, there are at most q^k such extensions with $\pi\in N_{L/K}(L^*)$.

Proof We note first that if $\alpha-\tau\alpha=u\alpha^{t+1}$, where u is a unit, then

$$h'(\alpha)=\prod_{i=1}^{p-1}(\alpha-\tau^i\alpha)\equiv -u^{-1}\alpha^{(t+1)(p-1)} \pmod{\alpha^{(t+1)(p-1)+1}} \tag{4}$$

nd

$$\alpha^p+(-1)^p\pi\equiv 0 \pmod{\pi\alpha}. \tag{5}$$

herefore if $v(h'(\alpha))=v(a_j)+(p-j-1)/p$, then we have

$$\begin{aligned}h'(\alpha)&\equiv(p-j)a_j\alpha^{p-j-1}\equiv -u^{p-1}\alpha^{(t+1)(p-1)}\\&\equiv -u^{p-1}\alpha^{kp+p-j-1} \pmod{\alpha^{(t+1)(p-1)+1}}\end{aligned}$$

hich is equivalent to

$$(p-j)a_j\equiv(-1)^p u^{p-1}\pi^k \pmod{\pi^{k+1}} \tag{6}$$

y (1), (4) and (5).

1) Let $L=K(\alpha)$, where α satisfies

$$h(X)=X^p+a_1X^{p-1}+\cdots+a_{p-1}X+(-1)^p\pi=0$$

ith

$$v(h'(\alpha))=v((p-j)a_j\alpha^{p-j-1}).$$

By Lemma 2 there are $\pmod{\pi^{k+r+1}}$

q^{r+1} choices for a_i, $i<j$,

q^r choices for a_i, $i>j$,

$q^r(q-1)/(p-1)$ choices for a_j,

ince a_j should satisy condition (6). Hence there are at most

$$\begin{aligned}&q^{(r+1)(j-1)}q^{r(p-j-1)}q^r(q-1)/(p-1)\\&=q^{r(p-1)+j-1}(q-1)/(p-1)=q^{k-1}(q-1)/(p-1)\end{aligned}$$

choices for $h(X)$.

2) If $[v(D(L/K)]=k=v(p)$, then $v(h'(\alpha))=v(p)+(p-1)/p=(p-1)(t+1)/p$, which forces $v(p)\equiv 0 \pmod{p-1}$.

If it is the case, then condition (4) and (5) implies that

$$p\equiv -u^{p-1}\pi^{k} \pmod{\pi^{k+1}}.$$

We have

$$q^{r} \text{ choices for } a_i,\ i\leqslant p-1,$$

modulo π^{k+r+1}. Hence there are at most $q^{r(p-1)}=q^{k}$ such extensions by Lemma 2.

Lemma 4. *Suppose that* char $K=0$, $v(p)=l$. *Let* $m=l+r+1$, *where* $r=(p-1)]$. *Then the group* $U/U^{p}U_m$ *has order* pq^{l} *or* q^{l} *according as* $-p\equiv X^{p-1}(\bmod\ \pi^{l}$ *has a solution or not.*

Proof Since every root of unit of degree $q-1$ is a p-th power, we have

$$U/U^{p}U_m\cong U_1/U_1^{p}U_m.$$

Define a mapping

$$\eta\colon U_1/U_m\to U_1/U_m$$
$$uU_m\to u^{p}U_m.$$

Then

$$|U_1/U_1^{p}U_m|=|\operatorname{coker}\eta|=|\ker\eta|.$$

Since

$$(1+\pi^{i}u)^{p}\equiv 1+\pi^{pi}u^{p} \pmod{\pi^{l+i}},$$

one sees that $i<r$ implies $U_i\backslash U_{i+1}$ is not in ker η. But $U_{r+1}\subset\ker\eta$.

For $i=r$ we have

$$\begin{aligned}(1+\pi^{r}u)^{p}&\equiv 1+p\pi^{r}u+\pi^{pr}u^{p}\\ &\equiv 1+\pi^{r}u(p+\pi^{(p-1)r}u^{p-1}) \pmod{\pi^{l+r+1}}.\end{aligned}$$

Therefore we have

$$|\ker\eta|=|U_{r+1}/U_m|=q^{l} \text{ if } p+(\pi^{r}u)^{p-1}\not\equiv 0 \pmod{\pi^{l+1}}.$$

When $p+(\pi^{r}u)^{p-1}\equiv 0 \pmod{\pi^{l+1}}$, one has

$$\ker\eta=\bigcup_{j=1}^{p-1}(1+u_0\pi^{r}\zeta^{i})U_{r+1}/U_m\ \cup\ U_{r+1}/U_m,$$

where ζ is a $(p-1)$ root of unit. Hence

$$|\ker\eta|=pq^{l}.$$

Proposition 2. *If* char $K=0$, *then every cyclic totally ramified extension* $L/$ *of degree* p *with* $\pi\in N_{L/K}(L^{*})$ *can be embedded into* $L_{\pi,m}$, *where*

$$m=v(p)+[v(p)/(p-1)]+1.$$

Proof 1) If $-p\equiv X^{p-1}(\bmod\ \pi^{l+1})$, where $l=v(p)$, has no solution.

There exist by Lemma 3 at most

$$\sum_{k=1}^{l}q^{k-1}(q-1)/(p-1)=(q^{l}-1)/(p-1)$$

totally ramified cyclic extensions L/K of degree p.

Let $E\subset L_{\pi,m}$ be the fixed field of the subgroup

$$\rho(U^p/U_m)\subset\rho(U/U_m)=\mathrm{Gal}(L_{\pi,m}/K).$$

Then $\mathrm{Gal}(E/K)\cong U/U^pU_m$, which is a group of type $(p, \cdots, p)$. Therefore every subgroup of U/U^pU_m of degree p corresponding to a subfield of degree p, which is totally ramified and has π as a norm. There are $(q^l-1)/(p-1)$ such subgroups because every such subgroup has $(p-1)$ elements of order p.

Hence there are, in this case, exact $(q^l-1)/(p-1)$ cyclic totally ramified extensions of degree p and all of them are contained in $L_{\pi,m}$.

2) If $-p\equiv X^{p-1}(\mathrm{mod}\ \pi^{l+1})$ has a solution.

There are by Lemma 3 at most

$$\sum_{k=1}^{l} q^{k-1}(q-1)/(p-1)+q^l=(q^l-1)/(p-1)+q^l=(pq^l-1)/(p-1)$$

such extensions.

On the other hand $L_{\pi,m}$ contains $(pq^l-1)/(p-1)$ such extensions since U/U^pU_m is of order pq^l by Lemma 4.

Corollary. *In case* Char $K=0$, *every equation*

$$h(X)=X^p+a_1X^{p-1}+\cdots+a_{p-1}X+(-1)^p\pi=0$$

defines a cyclic extension if $v(h'(\alpha))=v((p-j)a_j\alpha^{p-j-1})$ *and*

$$k=[v((p-j)a_j)]\equiv j(\mathrm{mod}\ p-1),\ \textit{and}$$

$$(p-j)a_j\equiv -X^{p-1}\pi^k\quad(\mathrm{mod}\ \pi^{k+1})$$

has a solution in K.

This corollary is interesting since it makes it possible to judge whether a polynomial is normal or not by the knowledge of its coefficients.

To deal with the case of char $K=p$, we need the following Lemma.

Lemma 5. *Let* $L_{\pi,m}$ *be a Lubin-Tate extension. Then*

$$v(D(L_{\pi,m}/K))=m-1/(q-1).$$

Proof It is easy to check that

$$v(D(L_{\pi,1}/K))=v((q-2)\lambda_1^{q-2})=1-1/(q-1),$$

$$v(D(L_{\pi,i}/L_{\pi,i-1}))=v(\pi)=1.$$

Lemma 6. *Let* L *be a subextension of degreee* p *of* $L_{\pi,m}/K$. *Then*

$$v(D(L/K))\leqslant m(p-1)/p.$$

Proof Let $G=\mathrm{Gal}(L_{\pi,m}/K))$ and let H be the subgroup of G keeping L fixed. Then $[G: H]=p$. Let G_i be the i-th ramification group of G. Then $G_{q^{m-1}}=(1)$ since

$$[1+\pi^ju]_F(\lambda_m)\equiv\lambda_m+[u]_F(\lambda_{m-j})\ \ (\mathrm{mod}\ \lambda_m\lambda_{m-j}),$$

which implies

$$\rho(1+\pi^ju)\,\overline{\in}\,G_{p^{m-1}}\ \text{if}\ j<m.$$

Let H_i be the i-th ramification group of H. Then we have

$$|H_i|\geqslant|G_i|/p.$$

since $H_i=G_i\cap H$. We have ([4] p. 64 or [5] p. 115)

$$v(D(L_{x,m}/K))=\frac{1}{q^{m-1}(q-1)}\sum_{i=0}^{q^{m-1}-1}(|G_i|-1).$$

On the other hand

$$v(D(L_{x,m}/K))=m-1/(q-1)$$

by Lemma 5. Hence

$$\begin{aligned}v(D(L_{x,m}/L))&=\frac{1}{q^{m-1}(q-1)}\sum_{i=0}^{q^{m-1}-1}(|H_i|-1)\\&\geqslant\frac{1}{q^{m-1}(q-1)}\sum_{i=0}^{q^{m-1}-1}\frac{|G_i|}{p}-1\\&=\left(m-\frac{1}{q-1}\right)\cdot\frac{1}{p}-\frac{p-1}{p}\,\frac{q^{m-1}}{q^{m-1}(q-1)}\\&=m/p-1/(q-1)\end{aligned}$$

and therefore

$$\begin{aligned}v(D(L/K))&=v(D(L_{x,m}/K))-v(D(L_{x,m}/L))\\&\leqslant m-1/(q-1)-(m/p-1/(q-1))=(p-1)m/p.\end{aligned}$$

Lemma 7. *Let K be of characteristic p. Then U/U_mU^p has order q^{m-r-1}, where $r=[(m-1)/p]$.*

Proof It is easy to see that $u\in U_1^pU_m$ if and only if n is of the form

$$u\equiv1+a_1\pi^p+a_2\pi^{2p}+\cdots+a_r\pi^{rp}\pmod{\pi^m}.$$

Hence $[U\colon U_mU^p]=[U_1\colon U_mU_1^p]=q^{m-r-1}$.

Proposition 3. *Let L/K be a cyclic totally ramified extension of degree p, where $p=$*char *K. Suppose*

$$v(D(L/K))=(p-1)m/p$$

and $\pi\in N_{L/K}(L^*)$. Then $E\subset L_{x,m}$.

Proof Let $l=[m(p-1)/p]$. Then $m=l+r+1$. There exist by Lemma 3 at most

$$\sum_{k=1}^{l}q^{k-1}(q-1)/(p-1)=(q^l-1)/(p-1)$$

cyclic totally ramified extensions of degree p with $v(D(L/K))\leqslant(p-1)m/p$ and with $\pi\in N_{L/K}(L^*)$. On the other hand there are

$$(q^{m-r-1}-1)/(p-1)=(q^l-1)/(p-1)$$

such extensions contained in $L_{x,m}$ by Lemmas 6 and 7.

Corollary. *In case* char *$K=p$, every equation*

$$h(X)=X^p+a_1X^{p-1}+\cdots+a_{p-1}X+(-1)^p\pi=0,\quad a_i\in\mathscr{M}$$

defines a cyclic extension if

$$ja_j\equiv-X^{p-1}\pi^k\pmod{\pi^{k+1}}$$

has a solution in K, where $k=v(a_j)$ and

$$v(a_j)+\frac{p-j-1}{p}=\min\left\{v(a_i)+\frac{p-i-1}{p}\right\}.$$

Proof It is clear by the proof of the proposition.

Combining Propositions 2 and 3 we get the following proposition.

Proposition 4. *Every cyclic totally ramified extension L/K of degree d, $d=p$ or $(d, p)=1$, has the embedding property and we have*

$$\ker R_L=N_{L/K}(L^*).$$

Proof It is clear by Propositions 2, 3 and 1.

§ 6. The Inequalities

In this section we prove the second inequality

$$[K^*: N_{L/K}(L^*)]\leqslant[L: K]$$

for any abelian extension L/K. On the other hand we prove the first inequality

$$[K^*: N_{L/K}(L^*)]\geqslant[L: K]$$

for subextensions L/K of generalized Lubin-Tate extensions. In the next section we prove that every abelian extension L/K can be embedded into a generalized Lubin-Tate extension and hence we get the first inequality.

Note first that both inequalities hold in the following cases:

1) $L=L_{\pi,m}\,E$, a generalized Lubin-Tate extension,

2) L/K is cyclic totally ramified extension of degree p or of degree d with $(d, p)=1$.

Indeed in these cases we have

$$\ker R_L=N_{L/K}(L^*).$$

Theorem 6. *Let L/K be any abelian extension. Then*

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

Proof We can find out subextensions

$$K=L\subset L_1\subset\cdots\subset L_r=L$$

such that L_{i+1}/L_i is cyclic of a prime degree. The extensions L_{i+1}/L_i fall into three cases:

1) L_{i+1}/L_i is unramified,

2) L_{i+1}/L_i is cyclic totally ramified of degree p,

3) L_{i+1}/L_i is cyclic totally ramified of degree d with $(d, p)=1$.

In all cases we have

$$[L_i^*: N_{L_{i+1}/L_i}(L_{i+1}^*)]=[L_{i+1}: L_i].$$

Hence

$$\begin{aligned}[K^*: N_{L/K}(L^*)]&\leqslant\prod_{i=1}^{r}[L_i^*: N_{L_{i+1}/L_i}(L_{i+1}^*)]\\&=\prod_{i=1}^{r}[L_{i+1}: L_i]=[L: K].\end{aligned}$$

Proposition 5. *Let L/K be a subextension of a generalized Lubin-Tate extension $L_{\pi,m}\,E/K$. Then*

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

Proof Let $M = L_{\pi,m}E$. Then we have by Theorem 6

$$[L^*: N_{M/L}(M^*)] \leqslant [M: L].$$

But

$$[K^*: N_{M/K}(M^*)] = [M: K].$$

Therefore

$$\begin{aligned}[M: K] &= [K^*: N_{M/K}(M^*)] \\ &\leqslant [K^*; N_{L/K}(L^*)]\,[L^*: N_{M/L}(M^*)] \\ &\leqslant [K^*: N_{L/K}(L^*)]\,[M: L],\end{aligned}$$

which implies

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

Combining this inequality with Theorem 6 one gets

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

Corollary. *Suppose L_1/K and L_2/K are two cyclic totally ramified extension o degree p. Let $L = L_1 \cdot L_2$. Then*

$$N_{L/K}(L^*) = N_{L_1/K}(L_2^*) \cap N_{L_2/K}(L_2^*).$$

Proof Since

$$[K^*: N_{L_1/K}(L_2^*)] = [K^*: N_{L_2/K}(L_2^*)] = p$$

by Proposition 4, we have

$$[K^*: N_{L_1/K}(L_2^*) \cap N_{L_2/K}(L_2^*]] \text{ divides } p^2.$$

It follows that there exists a prime $\pi \in N_{L_1/K}(L_2^*) \cap N_{L_2/K}(L_2^*)$. Hence L_1 and L_2 ca be embedded into $L_{\pi,m}$ for certain m by Proposition 4. Thereefore

$$L = L_1 \cdot L_2 \subset L_{\pi,m}.$$

Applying the proposition to L/K we get

$$[K^*: N_{L/K}(K^*)] = p^2,$$

if $L_1 \neq L_2$. The corollary follows from this and the fact that

$$N_{L/K}(L^*) \subset N_{L_1/K}(L_2^*) \cap N_{L_2/K}(L_2^*).$$

§7. Embedding Theorem II

In this section we prove that every totally ramified abelian extension L/K can be embedded into $L_{\pi,m}$ for certain m if π is in the norm of L^*. Class field theory for totally ramified case follows from this embedding theorem and Theorem 5.

If L/K is a totally ramified abelian extension, we can find subextensions L_i/K, $i=1, \cdots, r$, such that $\mathrm{Gal}(L_i/K)$ are all cyclic of degree $l_i^{\alpha_i}$ for some prime l_i and L is the composition of L_i, $i=1,\cdots,r$. Furthermore if $\pi \in N_{L/K}(L^*)$, then $\pi \in N_{L_i/K}(L_i^*)$. Therefore embedding L into $L_{\pi,m}$ is reduced to embedding L_i.

Lerma 8. *Suppose L/K is a cyclic totally ramified extension of degree p^r*

contained in $L_{\pi,m}$. There exists a cyclics subextension M/K of degree p^{r+1} in some $L_{\pi,n}$ such that $M \supset L$.

Proof Assume u is an element of $U(K)$ such that $R(u) \in \text{Gal}\ (L/K)$ has order p^r. Let n be the smallest integer such that $u^{p^r} \overline{\in} U_n$. Let H be the subgroup of U/U_n such that $R(H)$ has fixed field L. Hence $U/H \simeq \text{Gal}(L/K)$ and u is a generator of $\text{Gal}(L/K)$. Let H_2 be a maximum subgroup of H not containing the image of u^{p^r} and let M be fixd field of H_1. Then it is easy to see that M is that we required.

Theorem 7. *If L/K is a totally ramified abelian extension with $\pi \in N_{L/K}(L^*)$, then L is a subextension of $L_{\pi,m}$ for some m.*

Proof Without loss of generality we may assume L/K is cyclic of degree d, a power of a prime. If $(d, p)=1$, the theorem is proved already. Suppose $d=p^r$. The conclusion is true if $s=1$ (Proposition 4). By induction we may suppose the theorem is true for $d=p^{r-1}$, $r>1$.

Let L_1 be the subextension of degree p^{r-1}. Then $L_1 \subset L_{\pi,m_1}$, for some m_1. By Lemma 8 there exists a cyclic extension M/K of degree p^r such that $L_1 \subset M \subset L_{\pi,m_2}$ for certain m_2.

Let E be the composition of L and M.

If $L=M$, then the proof is finished.

Suppose $L \neq M$. Then $[E: L_1]=p^2$ and $[E: K]=p^{r+1}$. The extension E/K is not cyclic since it contains two different cyclic subextensions L and M of degree p^r. Therefore $\text{Gal}(E/K)$ is of type (p, p^r) since it has a cyclic factor group of order p^r. It follows that E contains a subextension N of degree p such that $E=L \cdot N=M \cdot N$.

If we can show that $\pi \in N_{E/K}(E^*)$, then $\pi \in N_{N/K}(N^*)$ and $N \subset L_{\pi,m_3}$ for some m_3. vThe theorem follows from the fact that $M \subset L_{\pi,m}$ and $N \subset L_{\pi,m}$ for

$$m \geqslant \max(m_2, m_3).$$

Indeed $\pi \in N_{E/K}(E^*)$. To show this we distinguish two cases.

Case 1. $$N_{L/K}(L^*)=M_{M/K}(L_1^*).$$

(In fact after finishing the proof we shall see that this case can not happen by Proposition 5.)

In this case we have

$$[K^*: N_{L/K}(L^*)]=p^{r-1},$$
$$[K^*: N_{E/K}(E^*)] \text{ divides } p^r.$$

But

$$[K^*: N_{M/K}(M^*)]=p^r,$$
$$N_{M/K}(M^*) \supset N_{E/K}(E^*).$$

Hence

$$\pi \in N_{M/K}(M^*)=N_{E/K}(E^*).$$

Case 2. $$N_{L/K}(L^*) \neq N_{M/K}(L_1^*).$$

In this case

$$[K^*: N_{L/K}(L_2^*)]=p^{r-1},$$
$$[K^*: N_{L/K}(L^*)]=p^r,$$
$$[L_1^*: N_{L_1/LK}(L^*)]-p$$

by Theorem 6 and Proposition 5.

If $\alpha\in L_1\backslash N_{L/L_1}(L^*)$, then

$$L_1=\bigcup_{i=0}^{p-1}\alpha^i N_{L/L_1}(L^*)$$

and

$$N_{L_1/K}(L_1^*)=\bigcup_{i=0}^{p-1}N_{L_1/K}(\alpha)^i N_{L/K}(L^*).$$

This implies that

$$N_{L_1/K}(\alpha)\neq\pi$$

since

$$\pi\in N_{L/K}(L^*).$$

Now let $\beta\in L_1$ be such that

$$N_{L_1/K}(\beta)=\pi,$$
$$\beta\in N_{M/L_1}(L_1^*).$$

Then

$$\beta\in N_{L/L_1}(L^*).$$

Hence it follows from Proposition 5, Corollary, that

$$N_{E/L_1}(E^*)=N_{L/L_1}(L^*)\cap N_{M/L_1}(M^*).$$

Therefore

$$\pi=N_{L_1/K}(\beta)\in N_{E/K}(E^*).$$

§ 8. Local Class Field Theory

In this section we prove that every abelian extension L/K can be embedde into a generalized Lubin-Tate extension $L_{\pi,m}$ E and the kernel of R is equal t $N_{L/K}(L^*)$.

First we deal with the case of a cyclic extension.

Lemma 9. *Let L/K be a cyclic extension of degree d. Then there exists a unramified extension E and a totally ramified extension M such that $L\subset M\cdot E$ Furthermore we can choose E so that $[E: K]=1$ or d according as L/K is totall ramified or not and choose M so that $[M: K]=[L: K_L]$, where K_L is the maxima unramified subextension of L.*

Proof The lemma is trivial if L/K is totally ramified or unramified. Suppos $K\subsetneq K_L\subsetneq L$. Let E be the unramified extension of degree d. Let $N=E\cdot L$. Let $\sigma\in\mathrm{Gal}(N/K)$ be an automorphism such that $\sigma|_E=$Frobenius substitution. Let M b the fixed field of σ. Then it is not difficult to see that $L\cdot M=N$ and M is totally ramified with required degree.

Theorem 8. *Every abelian extension L/K can be embedded into certian* *generalized extension* $L_{x,m}\cdot E$.

Proof By Lemma 9 the theorem is true for any cyclic extension. But L is a composition of cyclic subextensions L_i. Hence $L_i\subset L_{\pi_i,m_i}\cdot E_i$. Taking E and m big enough we have $L_{\pi_i,m_i}\subset L_{\pi,m}\ E$ by Theorem 2.

Let L/K be as above. We define E, M and N by the last lemma. We have reciprocity map R_N: $K^*\to\mathrm{Gal}(N/K)$. On the other hand, viewing K_L as a base field we can define another reciprocity R'_N: $K^*_L\to\mathrm{Gal}(N/K_L)$. We can identify $R'_N(K^*_L)$ with a subgroup of $R_N(K^*)$. We want to find out the relationship between R_N and R'_N.

Lemma 10. *Let L/K be a totally ramified cyclic extension with Galois group $G=\mathrm{Gal}(L/K)$. Let $v=\{\tau u/u|\tau\in G.\ u\in U(L)\}$ and $U=U(L)$. Define a mapping*

$$\eta\colon G\to U/V$$

by

$$\tau\to\tau\pi_L/\pi_L\cdot V.$$

Then η is an injective group homomorphism independent of the choice of π_L.

Proof Let π'_L be another uniformizing element of L. Then $\pi'_L=\pi_L v$ for some $v\in U$. Hence

$$\tau\pi'_L/\pi'_L=\tau\pi_L\cdot\tau v/\pi_L\cdot v\in\tau\pi_L/\pi_L\cdot v,$$

so η is independent of the choice of π_L.

If $\rho\in G$, then

$$(\rho\tau)\pi_L/\pi_L=\rho(\tau\pi_L)/\tau\pi_L\cdot\tau\pi_L/\pi_L\in\rho\pi_L/\pi_L\cdot\tau\pi_L/\pi_L\cdot v.$$

Hence η is a group homomorphism.

If $\tau\pi_L/\pi_L\in V$, let ρ be a generator of G and suppose $\tau=\rho^r$. Then

$$\tau\pi_L/\pi_L=\prod_{i=1}^{l}\ \rho^i u_i/u_i=\rho\ u/u,$$

where u is an element of U. It follows that

$$\rho u/u=\rho^r\pi_L/\pi_L=\rho((\rho^{r-1}\pi_L)(\rho^{r-2}\pi_L)\cdots(\tau_L)/(\rho^{r-1}\pi_L)\cdots\pi_L,$$

which implies $u^{-1}(\rho^{r-1}\pi_L)\cdots(\rho\pi_L)\pi_L$ is fixed by ρ and hence is in K. But $v(\pi_L)=1/d$, where $d=[L\colon K]$ since L/K is totally ramified. Therefore $d|\mathrm{r}$ and $\tau=\rho^r=id$.

Propotition 6. *Let L/K be a cyclic extension. Then* $\ker R_L=N_{L/K}(L^*)$.

The proof follows [2] with slight modification.

Proof By Lemma 9 and Theorem 7, L can be embedded into some Lubin-Tate extension and hence the first and second inequalities hold by Proposition 5. So we need only to show that

$$\ker R_L\supset N_{L/K}(L^*).$$

Let M, N and E be as in Lemma 9, i. e., M is totally ramified of degree equal to $e(L/K)$, and E is unramified of degree $n=[L\colon K]$ and $N=E\cdot M=M\cdot L=E\cdot L$. Let K_L be the maximal unramified subextension of L.

We have

$$[M: K]=[M': K_L]=[L: K_L]=[E: K_L]=e,$$
$$[K_L: K]=f.$$
$$[L: K]=[E: K]=n=ef.$$

Let α be a uniformizing element of M such that
$$N_{M/K}(\alpha)=N_{N/E}(\alpha)=\pi.$$

Let $$\Pi=\{\pi'\in N_{L/K_L}(L^*)\,|\,v(\pi')=1\}.$$

The set Π generates the group $N_{L/K_L}(L^*)$. It is enough to show that
$$R(N_{K_L/K}(\pi')\,|)_L=id.$$

Let σ be the Frobenius substitution of E/K. Then σ^f is the Frobeniu substitution of E/K_L.

We define the reciprocity map of N/K_L
$$R': K_L^*\to \mathrm{Gal}(N/K_L).$$

Then
$$R'(\pi')\,|_L=id \text{ for } \pi'\in\Pi.$$

Therefore we need only to show that
$$R(N_{K_L/K}(\pi'))=R'(\pi').$$

Let $\pi'\in\Pi$. Then $\pi'=N_{L/K_L}(\alpha X)$ for some $x\in U(N)$ such that $\alpha x\in L$. Then
$$N_{N/E}(\alpha x)=\pi.\ N_{N/E}(x)=\pi u,$$
where $u=N_{N/E}(x)$. It turns out that
$$R'(\pi)(\alpha)=\alpha$$
since $\pi=N_{M'/K_L}(\alpha)$ and M'/K_L is totally ramified.

It follows from
$$R'(\pi)(\alpha)-\alpha,$$
$$R'(\pi u)(\alpha x)=ax$$
that
$$\frac{R'(u)\alpha}{\alpha}=\frac{x}{R'(\pi u)x}. \tag{7}$$

Let $$v=N_{K_L/K}(u)=u(\sigma u)\cdots(\sigma^{f-1}u)$$
and $$Y=x(\sigma x)\cdots(\sigma^{f-1}x)$$
where $\sigma\alpha=\alpha$ and $\sigma|_E$ is the Frobenius mapping. One has
$$R'(\pi)=\sigma^f=(R(\pi))^f=R(\pi^f)=R(N_{K_L/K}(\pi)).$$

Hence the proposition is proved if we can show that $R(v)=R'(u)$. But
$$R(v)\,|_E=id=R'(u)\,|_E.$$

It is enough to show that
$$R(v)\alpha=R'(u)\alpha.$$

It follows from (7) that
$$\frac{R'(u)\alpha}{\alpha}=\frac{x}{R'(\pi u)x}=\frac{x}{R'(u)\sigma^f x}=\frac{x(\sigma x)\cdots(\sigma^{f-1}x)}{(\sigma x)\cdots(\sigma^f x)}\cdot\frac{f_x}{R'(u)\sigma^f x}$$
$$=\frac{y}{\sigma y}\,\frac{\sigma^f x}{R^f(u)\sigma^f x}\equiv\frac{y}{\sigma y}\quad\bmod V, \tag{8}$$

where V is defined as in Lemma 10 for N/E.

On the other hand the fixed field of $R(\pi v)$ is totally ramified. It is generated by some β with $N_{N/E}(\beta)=\pi v$. Let $\beta=\alpha z$, where $z\in U(N)$. Then

$$R(\pi v)\beta=R(\pi v)\alpha z=\alpha z=\beta.$$

Hence

$$\frac{R(v)\alpha}{\alpha}=\frac{z}{R(\pi v)z}=\frac{z}{R(v)\sigma z}\equiv\frac{z}{\sigma z}\pmod{V}. \qquad (9)$$

We need only to show that

$$\frac{z}{\sigma z}\equiv\frac{y}{\sigma y}\pmod{V}$$

by Lemma 10 and equations (8) and (9). But

$$N_{N/E}(z)=N_{N/E}(y)=v.$$

It follows from Hilbert 90 that

$$\frac{y}{z}=\frac{\tau\alpha^j w}{\alpha^j w},$$

where τ is a generator of $\mathrm{Gal}(N/E)$ and $w\in U(N)$. Hence

$$\frac{z}{\sigma z}=\frac{y}{\sigma y}\cdot\frac{\tau\alpha^j w}{\alpha^j w}\cdot\frac{\sigma\alpha^j w}{\sigma\tau\alpha^j w}=\frac{y}{\sigma y}\cdot\frac{\tau w}{w}\cdot\frac{\sigma w}{\tau\sigma w}\equiv\frac{y}{\sigma y}\pmod{V}$$

since $\sigma\alpha=\alpha$.

Theorem 9. *Let L/K be an abelian extension. Then the kernel of the reciprocity map is equal to $N_{L/K}(L^*)$.*

Proof We need only to show that

$$\ker R\supset N_{L/K}(L^*)$$

since $[K^*:\ker R]=[K^*: N_{L/K}(L^*)]$. Let $L_1, \cdots, L_s$ be cyclic subextensions of L such that L is the composition of L_i. Then

$$N_{L/K}(L^*)\subset N_{L_i/K}(L^*) \quad \text{for } i=1, \cdots, s.$$

For any $x\in N_{L/K}(L^*)$ we have by Proposition 6

$$R(x)\,|_{L_i}=id.,$$

which implies $R(x)=id.$, since L is the composition of L_i, $i=1, \cdots, s$.

References

[1] Hazewinkel, M., Formal Groups and Applications, Academic Press, New York, 1978.
[2] Hazewinkel, M., Local class field theory is easy, *Advances in Math.*, **18** (1975), 148—181.
[3] Lubin, J. & Tate, J., Formal complex multiplication in local fields, *Ann. Math.*, **81** (1965), 380—387.
[4] Serre, J. P., *Corps Locaux, Hermann*, Paris, 1962.
[5] Weiss, E., Algebraic Numbea Theory, McGraw-Hill, New York, 1963.