ERASMUS UNIVERSITEIT ROTTERDAM
Nederlandse Economische Hogeschool
ECONOMETRISCH INSTITUUT (Dept. Math)

Report 7318/M

LOCAL CLASS FIELD THEORY IS EASY

Michiel Hazewinkel

Oct. 3, 1973

LOCAL CLASS FIELD THEORY IS EASY *)

Michiel Hazewinkel

Contents

1. INTRODUCTION

Let K be a local field with finite residue field. "Local class field theory", for the purposes of this paper consists of the (more or less) explicit description of the maximal abelian extension K_{ab} of K, of the calculation of the galois group $\mathrm{Gal}(K_{ab}/K)$; i.e. the proof that $\mathrm{Gal}(K_{ab}/K) \simeq \hat{K}^*$, the completion of K^* with respect to the topology given by the open subgroups of finite index in K^*, and finally of a description of the isomorphism $\hat{K}^* \xrightarrow{\sim} \mathrm{Gal}(K_{ab}/K)$. "Local class field theory" in this paper does not indude e.g. a calculation of the Brauer group $\mathrm{Br}(K)$.

It is the aim of this paper, which is partly expository in nature, to show that "local class field theory" in this sense can be treated in a fairly small number of pages (38) and without using any of the involved (but powerfull) machinery which one "usually" finds in this connection. In particular we need nothing at all (not even in a concealed way) of the cohomology of groups. All the facts which we assume known are collected in §2. A large part of this paper (§3, 5, 6 and most of §7) is closely related to my 1969 amsterdam thesis.

---

*) Part of the work for this paper was done while the author enjoyed a Fullbright-Hays travelling grant (Febr/March 1973).

The remaining part of this introduction consists of an outline of the structure of the theory.

First let K be a local field with algebraically closed residue field, and let L/K be an abelian (necessarily totally ramified) extension of K. Then one forms the following sequence.

$$(1.1) \qquad 0 \to \mathrm{Gal}(L/K) \xrightarrow{i} U(L)/V(L/K) \xrightarrow{N} U(K) \to 0$$

where U(L), U(K) are the units of L and K respectively; V(L/K) is the subgroup of U(L) generated by the elements of the form $s(u)u^{-1}$, $u \in U(L)$, $s \in \mathrm{Gal}(L/K)$; the homomorphism i associates the class of $s(\pi_L)(\pi_L)^{-1}$ to $s \in \mathrm{Gal}(L/K)$, where π_L is a uniformizing element of L; and N is induced by the norm map $N_{L/K}$.

The first main result on which the theory rests is

(1.2) Theorem. The sequence (1.1) is exact.

The proof of this theorem (cf. §4) presented here, is, as far as I know, completely new. The old proof in [4] still used some cohomology of groups theory.

Next, let K be a local field with finite residue field and L/K an abelian extension of K. Taking maximal unramified extensions and completing them we obtain an abelian extension of local fields with algebraically closed residue fields $\hat{L}_{nr}/\hat{K}_{nr}$ with galoisgroup $\mathrm{Gal}(\hat{L}_{nr}/\hat{K}_{nr})$ canonically isomorphic to $\mathrm{Gal}(L/K)_{ram}$, the ramification subgroup of Gal(L/K). We can now form the diagram with exact rows.

$$\begin{array}{ccccccccc}
0 \to & \mathrm{Gal}(L/K)_{ram} & \longrightarrow & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) & \longrightarrow & U(\hat{K}_{nr}) & \to 0 \\
& \downarrow F-1 & & \downarrow F-1 & & \downarrow F-1 & \\
0 \to & \mathrm{Gal}(L/K)_{ram} & \longrightarrow & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) & \longrightarrow & U(\hat{K}_{nr}) & \to 0
\end{array}$$

where F is a lift of the Frobenius automorphism $F \in \mathrm{Gal}(k_s/k)$, k_s the algebraic closure of k. Because $\mathrm{Ker}(F-1: U(\hat{K}_{nr}) \to U(\hat{K}_{nr}) = U(K)$ and the induced map $F-1: \mathrm{Gal}(K/K)_{ram} \to \mathrm{Gal}(L/K)_{ram}$ is the zero map, we obtain by means of the snake lemma a homomorphism

$$\phi(L/K) : U(K) \to \mathrm{Gal}(L/K)_{ram}.$$

This homomorphism turns out to be surjective and its kernel is $N_{L/K}U(L)$. It is also functorial in L. These homomorphisms then look remarkably like part of the "reciprocity homomorphisms" $r(L/K) : K^* \to \mathrm{Gal}(L/K)$ which we are trying to construct.

The next step is to construct a number of abelian totally ramified extensions L_m/K which have maximally small norm groups. These are the Lubin-Tate extensions first constructed in [7]. In case $K = Q_p$ they are the extensions generated by the p-th roots of unity.

They are obtained as follows. Choose a uniformizing element π_K of K. Let f(X) be a polynomial of the form $f(X) = X^q + \pi_K(a_{q-1}X^{q-1} + \ldots + a_2 X^2) + \pi_K X$, where $a_i \in A(K)$, the integers of K, and q is the number of elements of k, the residue field of K. Let $f^{(m)}(X)$ be inductively defined as $f^{(m)}(X) = f(f^{(m-1)}(X))$ and let λ_m be a root of $f^{(m)}(X)$ which is not a root of $f^{(m-1)}(X)$. One defines $L_m = K(\lambda_m)$. One now proves

(1.3) Theorem. (i) $N_{L_m/K}(U(L_m)) \subset U^m(K) = \{u \in U(K) \mid u \equiv 1 \bmod \pi_K^m\}$.

(ii) L_m/K is an abelian totally ramified extension of degree $(q-1)q^{m-1}$.

The "almost reciprocity homomorphism" then gives $N_{L_m/K}(U(L_m)) = U^m(K)$, and using this (and the fact that $\mathrm{Gal}(K_{nr}/K) = \hat{Z}$ is topologically free) the "almost reciprocity homomorphism" yields that $\mathrm{Gal}(K_{ab}/K) \simeq U(K) \times \hat{Z}$ and that $K_{ab} = L_\pi . K_{nr}$, where $L_\pi = \bigcup_m L_m$. It remains to "extend" the "almost reciprocity homomorphism" $\phi: U(K) \to \mathrm{Gal}(K_{ab}/K)_{ram}$ to a reciprocity homomorphism $r : K^* \to \mathrm{Gal}(K_{ab}/K)$ such that the kernel of $r: K^* \to \mathrm{Gal}(K_{ab}/K) \to \mathrm{Gal}(L/K)$ is precisely $N_{L/K}(L^*)$ for abelian extensions L/K. It turns out that the map $u \mapsto \phi(u^{-1})$ can indeed be extended in this way.

Finally we give the "explicit" description of $r : K^* \to \mathrm{Gal}(K_{ab}/K)$, due to Lubin and Tate. This final part of §7 is based on [7].

Over the years I have had many valuable conversations with various people about "local class field theory". It remains for me to thank them, especially Dr. A. Menalda (to whom I owe a main part of the idea of the proof of (1.3) (ii)), Prof. J. Neukirch (who challenged me to get rid of all cohomological considerations), Prof. F. Oort, and the many people who urged me to write this stuff down.

2. PRECIS OF NOTATIONS, CONVENTIONS AND RESULTS ASSUMED KNOWN.

In this section we have collected the results without proofs which will be used in the following. They can all be found in a standard text like [8], Parts I, II and [9].

2.1. Notations (for local fields)

A local field K is a field K with a (normalized exponential) valuation $v_K : K^* \to Z$ on it. We define:

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

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

π_K, a uniformizing element of K; i.e. an element of K such that $v_K(\pi_K) = 1$.

$\mathfrak{m}(K) = \{x \in K \mid v_K(x) > 0\} = \pi_K A(K)$, the maximal ideal of A(K).

$U^m(K) = \{x \in U(K) \mid x \equiv 1 \bmod (\pi_K^m)\}$.

$k = A(K)/\mathfrak{m}(K)$, the residue field of K. We shall always assume that k is perfect.

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

Finally $\#S$ denotes the number of elements of a set S.

2.2. Extensions of local fields

Let L/K be a finite galois extension. The galois group is denoted Gal(L/K). This is a solvable group if the residue field is finite or algebraically closed. Cf. [8] Ch. IV §2. (If L/K is not galois one denotes with $\Gamma(K, L \to \Omega)$ the various isomorphisms of L into a (large enough) algebraically closed field Ω). Let K_L be the maximal unramified subextension of L/K. The subgroup $Gal(L,K_L)$ is denoted $Gal(L/K)_{ram}$ and is called the ramification subgroup of Gal(L/K). $Gal(L/K)_{ram}$ is a normal subgroup of Gal(L/K). If M/K is a galois extension containing L/K then the natural map $Gal(M/K) \to Gal(L/K)$ maps $Gal(M/K)_{ram}$ into $Gal(L/K)_{ram}$.

Let K_{nr} be a maximal unramified extension of K. The completion $\hat{K}_{nr}$, is a local field with as residue field k_s, an algebraic closure of k. We now choose once and for all an algebraically closed extension Ω of $\hat{K}_{nr}$ and all extensions of K are supposed to be contained in Ω. If k is finite, then $Gal(K_{nr}/K) = \hat{Z}$ (the completion of Z with respect to the topology of subgroups of finite index), and we use F to denote the Frobenius automorphism in $Gal(k_s/k)$, to denote its canonical lift in $Gal(K_{nr}/K)$ and its extension to a K-automorphism of $\hat{K}_{nr}$.

K_{ab} denotes the maximal abelian extension of K. If k is finite $K_{nr} \subset K_{ab}$.

If L/K is finite galois, then $\hat{L}_{nr}/\hat{K}_{nr}$ is a galois extension with its galois group $Gal(\hat{L}_{nr}/\hat{K}_{nr})$ canonically isomorphic to $Gal(L/K)_{ram}$ (restrict $s \in Gal(\hat{L}_{nr}/\hat{K}_{nr})$ to L).

2.3. Two results on norm maps.

(i) Let K be a local field with algebraically closed residue field, and L/K a finite extension of K. Then $N_{L/K}: L^* \to K^*$ and $N_{L/K}: U(L) \to U(K)$ are surjective (Cf.[8] Ch. V).

(ii) Let K be a local field with finite residue field and L/K an unramified galois extension then $N_{L/K}: U(L) \to U(K)$ is surjective (Cf.[8] Ch. V §2).

3. THE DECOMPOSITION THEOREM

Let K be a local field (in the sense of §2). We fix some algebraically closed field Ω containing $\hat{K}_{nr}$. All composite fields are supposed to be taken in this large field.

(3.1.) Theorem.

Let L/K be a finite galois extension, where K is a local field with

finite residue field. Then there is a totally ramified extension L'/K such that $L'_{nr} = L'.K_{nr} = L.K_{nr} = L_{nr}$. If $\mathrm{Gal}(L/K)_{ram} \subset Z\mathrm{Gal}(L/K)$ we can take L'/K to be an (abelian) galois extension.
(Here ZG denotes the centre of the group G).

Proof. Let K_L be the maximal unramified subextension of L/K.

The galois group $\mathrm{Gal}(K_L/K)$ is cyclic with F (Frobenius) as a generator. Let F' be any lift in $\mathrm{Gal}(L/K)$ of F. Let r be the order of F'. Let K_r be the unramified extension of degree r of K. Then $K_L \subset K_r$. Define $F'' \in \mathrm{Gal}(L.K_r/K)$ by means of the conditions $F''|K_r$ = Frobenius $\in \mathrm{Gal}(K_r/K)$ and $F''|_L = F' \in \mathrm{Gal}(L/K)$. Then F'' is welldefined. Let

$$\begin{array}{ccc} & & L \\ & & \Big| \\ K & \text{———} & K_L \end{array}$$

L' be the invariant field of F''. Then L'/K is totally ramified and $L'.K_r = L.K_r$.

Finally if $\mathrm{Gal}(L/K)_{ram} \subset Z\mathrm{Gal}(L/K)$, then $G(L.K_r/K)_{ram} \subset Z\mathrm{Gal}(L.K_r/K)$ which implies that the subgroup of $\mathrm{Gal}(L.K_r/K)$ generated by F'' is normal, so that L' is galois over K.

(3.2.) Remark.

Theorem (3.1) is also true for local fields K with perfect (but not necessarily finite) residue fields. Cf. [4], 2.8 or [5], no.2. The proof is different in those cases.

(3.3.) Corollary.

Let K_{ab} be the maximal abelian extension of K. Then $K_{ab} = K_{nr}.L$ where L/K is a maximal totally ramified abelian extension of K.

Proof. Use infinite galois theory and the fact that $\mathrm{Gal}(K_{nr}/K) \simeq \hat{Z}$ is topologically free.

(3.4) Corollary.

$\mathrm{Gal}(K_{ab}/K)_{ram} = \varprojlim \mathrm{Gal}(L/K)_{ram}$ where L/K runs over all finite abelian extensions and the maps $\mathrm{Gal}(L/K)_{ram} \to \mathrm{Gal}(M/K)_{ram}$ are induced by the natural projections $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ if $M \subset L$;
$\mathrm{Gal}(K_{ab}/K) \simeq \mathrm{Gal}(K_{ab}/K)_{ram} \times \hat{Z}$.

4. LOCAL FIELDS WITH ALGEBRAICALLY CLOSED RESIDUE FIELD.

In this section K is a local field with algebraically closed residue field.

(4.1) Let L/K be an abelian galois extension (necessarily totally ramified). We consider the following sequence of abelian groups

$$(4.1.1) \qquad 0 \to \mathrm{Gal}(L/K) \xrightarrow{i} U(L)/V(L/K) \xrightarrow{N_{L/K}} U(K) \to 0$$

where $U(L)$ is the group of units of L; $U(K)$ is the group of units of K; $V(L/K)$ is the subgroup of $U(L)$ generated by the elements of the form $\frac{su}{u}$, $u \in U(L)$, $s \in \mathrm{Gal}(L/K)$; $N_{L/K}$ is induced by the norm map $U(L) \to U(K)$ (It is clear that $N_{L/K}(V(L/K)) = \{1\}$); and i is defined as $i(s) = \text{class of } \frac{s\pi_L}{\pi_L}$ (this does not depend on the choice of π_L).

(4.2) Lemma.

The map i is a homomorphism of groups

Proof. $$\frac{st(\pi_L)}{\pi_L} = \frac{s(t(\pi_L))}{t(\pi_L)} \cdot \frac{t(\pi_L)}{\pi_L} \equiv \frac{s(\pi_L)}{\pi_L} \cdot \frac{t(\pi_L)}{\pi_L} \bmod V(L/K)$$

because $t(\pi_L)$ is another uniformizing element of L; i.e. $t(\pi_L) = u\pi_L$ for a certain $u \in U(L)$.

(4.3) Theorem on the fundamental exact sequence.

Let L/K be an abelian extension of the local field K (with algebraically closed residue field). Then the sequence (4.1.1)

$$0 \to \mathrm{Gal}(L/K) \xrightarrow{i} U(L)/V(L/K) \to U(K) \to 0$$

is exact. This sequence will be called the fundamental exact sequence.

The proof of theorem (4.3) is divided into several steps. We first prove the injectivity of i. To do this we use the following elementary lemma on abelian groups.

(4.4) Lemma.

Let G be a finite abelian group and $g \in G$ an element of G. Then there exists a subgroup H of G such that the following conditions are fulfilled

(i) G/H is cyclic

(ii) If $r : G \to G/H$ is the canonical map, then $\mathrm{ord}(g) = \mathrm{ord}(r(g))$ where $\mathrm{ord}(\ )$ denotes the order of a group element.

Proof. Let $g = \oplus G_p$ be the decomposition of G into its Sylow subgroups, and let $g = (g_p)_p$ under this decomposition. We write G_p as a direct sum of cyclic groups

$$G_p = Z/(p^{i_1}) \oplus \ldots \oplus Z/(p^{i_r}), \qquad g_p = (g_p(1),\ldots,g_p(r)),$$

For $n \in Z$, let $v_p(n)$ denote the number of factors p in n; i.e. $n = p^{v_p(n)}.m$ with $(p,m) = 1$ and let

$$w_p(g_p) = \max_n \{i_n - v_p(g_p(n))\}$$

Then

$$\mathrm{ord}(g_p) = p^{w_p(g_p)}$$

Now choose an index b such that $w_p(g_p) = i_b - v_p(g_p(b))$. And let

$$H_p = \bigoplus_{i_n \neq b} Z/(p^{i_n}) \subset G_p$$

$$H = \oplus H_p \subset G$$

Then if $r_p : G_p \to G_p/H_p$ is the canonical map, $\mathrm{ord}(g_p) = \mathrm{ord}(r_p(g_p))$ and consequently $\mathrm{ord}(g) = \mathrm{ord}(r(g))$

(4.5) Proof of the injectivity of $i : \mathrm{Gal}(L/K) \to U(L)/V(L/K)$

Let $1 \neq g \in G = \mathrm{Gal}(L/K)$; and let H be a subgroup of G such that the two assertions of (4.4) hold. Let $\bar{g}$ be the image of g in G/H, then $\bar{g} \neq 1$; let $\bar{f}$ be a generator of G/H and let f be any lift in G of $\bar{f}$; then if $\bar{g} = \bar{f}^r$

$$g = f^r h \qquad \text{for a certain } h \in H.$$

Suppose that $i(g) \in V(L/K)$. Then we have (using(4.2))

$$(4.5.1) \qquad \frac{f(\pi_L^r)}{\pi_L^r} \cdot \frac{h(\pi_L)}{\pi_L} = \prod_{i,j} \frac{f^i h_j(u_{ij})}{u_{ij}}$$

where $i = 1,2,\dots,\mathrm{ord}(f)$; and h_j runs through the elements of H; and $u_{ij} \in U(L)$.

Now because

$$(4.5.2) \qquad \frac{f^i h(u)}{u} = \frac{f^i h(u)}{f^{i-1}h(u)} \cdot \frac{f^{i-1}h(u)}{f^{i-2}h(u)} \cdots \frac{f^2h(u)}{fh(u)} \cdot \frac{fh(u)}{h(u)} \cdot \frac{h(u)}{u}$$

we can rewrite (4.5.1) as

$$(4.5.3) \qquad \frac{f(\pi_L^r)}{\pi_L^r} \cdot \frac{h(\pi_L)}{\pi_L} = \frac{f(w)}{w} \cdot \prod_{h\in H} \frac{h(u_h)}{u_h} \qquad w \in U(L),\ u_h \in U(L)$$

Let M be the invariant field of the subgroup H of G. Taking $N_{L/M}$ on both sides of equation (4.5.3) we obtain

$$(4.5.4) \qquad \frac{\bar{f}(\pi_M^r)}{\pi_M^r} = \frac{\bar{f}(\bar{w})}{\bar{w}}$$

where $\pi_M = N_{L/M}(\pi_L)$ and $\bar{w} = N_{L/M}(w)$. Because M/K is cyclic, equation (4.5.4) implies that $\pi_M^r \bar{w}^{-1} \in K$, which is impossible because M/K is totally ramified and $r < \mathrm{ord}(\bar{f}) = [M : K]$, as $\bar{g} \neq 1$.

The second step of the proof of theorem (4.3) consists of the proof of the exactness of the fundamental sequence in the case that L/K is a cyclic extension. To do this we need the "classical" version of "Hibert 90" (cf.[3], §13, Satz 114).

We repeat the proof for completeness sake.

4.6. Lemma.("Hilbert 90")

Let L/K be a cyclic galois extension, and suppose that $N_{L/K}(x) = 1$ for a certain $x \in L$. Then there exists an $y \in L$ such that

$x = \frac{sy}{y}$, where $s \in \mathrm{Gal}(L/K)$ is a generator of the galois group.

<u>Proof</u>. Let a be any element of L. One forms

$$y = a + s(a)x^{-1} + s^2(a).s(x^{-1}).x^{-1} + \ldots + s^{n-1}(a).s^{n-2}(x^{-1})\ldots s(x^{-1}).x^{-1}$$

where n = ord(s). We then have

$$s(y) = s(a) + s^2(a)s(x^{-1}) + \ldots + s^{n-1}(a).s^{n-2}(x^{-1})\ldots s(x^{-1}) + $$
$$+ s^n(a).s^{n-1}(x^{-1})\ldots s(x^{-1})$$

As $s^n(a) = a$ and $s^{n-1}(x^{-1})\ldots s(x^{-1})x^{-1} = 1$, it follows that

$$s(y)x^{-1} = y$$

If y were equal to zero for all a; then letting a run through a basis of L over K we would have a nontrivial solution (viz. $(1, x^{-1}, s(x^{-1})x^{-1}, \ldots s^{n-2}(x^{-1})\ldots s(x^{-1})x^{-1})$ for an nxn system of linear equations with nonzero determinant. Therefore $y \neq 0$ for suitable a, which means that $x = s(y)y^{-1}$.

(4.7) <u>Proof of the exactness of the fundamental exact sequence in the cyclic case</u>

Let L/K be a cyclic extension. We consider

$$(4.7.1) \qquad 0 \to \mathrm{Gal}(L/K) \xrightarrow{i} U(L)/V(L/K) \xrightarrow{N} U(K) \to 0$$

The injectivity of i has just been proved. The surjectivity of N is very well-known. Cf. (2.3). It remains to prove that KerN = Imi. That $N \circ i$ is the zero map is obvious. Suppose then that $N(u) = 1$. According to Lemma 4.6 there is an $y \in L^*$ such that $u = s(y)y^{-1}$, where s is a generator of Gal(L/K). Write $y = \pi_L^r v$. Then

$$u \equiv \frac{s(\pi_L^r)}{\pi_L^r} \equiv \frac{s^r(\pi_L)}{\pi_L} \mod V(L/K)$$

which concludes the proof.

The next step (the third) of the proof of theorem 4.3 consists of two easy technical lemmata.

(4.8) Lemma.

Let L/K be a finite galois extension, and M a sub galois extension of L. Then the induced map

$$N_{L/M} : V(L/K) \to V(M/K)$$

is surjective.

Proof. Let H be the subgroup of $G = \mathrm{Gal}(L/K)$ corresponding to M. It suffices to show that $\frac{\bar{g}(u)}{u} \in \mathrm{Im}\, N_{L/M}$ for $\bar{g} \in G/H$ and $u \in U(M)$. Because $N_{L/M} : U(L) \to U(M)$ is surjective there is an $v \in U(L)$ such that $N_{L/M}(v) = u$. Let $g \in G$ be any lift of $\bar{g}$.

Then

$$N_{L/M}\left(\frac{g(v)}{v}\right) = \prod_{h \in H} \frac{hg(v)}{h(v)} = \frac{\prod g(g^{-1}hg)(v)}{\prod h(v)} = \frac{\bar{g}(u)}{u}$$

which proves the lemma.

(4.9) Lemma.

Let L/K be a finite galois extension, and M a subextension of L such that L/M is cyclic. Then the following sequence is exact

$$0 \to \mathrm{Gal}(L/M) \xrightarrow{i} U(L)/V(L/K) \xrightarrow{N} U(M)/V(M)K) \to 0$$

Proof. i is injective because $\mathrm{Gal}(L/M)$ is a subgroup of $\mathrm{Gal}(L/K)$. Cf. (4.5); and N is surjective because $N : U(L) \to U(M)$ is surjective. Now consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(L/M) \arrow[r, "i"] \arrow[d, equal] & U(L)/V(L/M) \arrow[r, "N"] \arrow[d] & U(M) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Gal}(L/M) \arrow[r, "i"] & U(L)/V(L/K) \arrow[r, "N"] & U(M)/V(M/K) \arrow[r] & 0
\end{tikzcd}$$

where the two arrows in the middle and on the right are natural projections. Let $u \in U(L)$ and suppose $N(u) \in V(M/K)$. Because of lemma (4.8) there is a $v \in V(L/K)$ such that $N(v) = N(u)$, i.e. $N(uv^{-1}) = 1$. Using exactness of the top line (4.7) we obtain that $uv^{-1} \equiv s(\pi_L)/\pi_L \mod V(L/M)$ for a certain $s \in \mathrm{Gal}(L/M)$ which implies $u \equiv s(\pi_L)\pi_L^{-1} \mod V(L/K)$. This proves the lemma.

The final step in the proof of Theorem 4.3 is an induction argument.

(4.10) Proof of theorem 4.3.

Let L/K be an abelian extension; M/K a subextension such that L/M is cyclic. By induction we can assume that the fundamental sequence for M/K is exact. Now consider the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathrm{Gal}(L/M) & = & \mathrm{Gal}(L/M) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & \mathrm{Gal}(L/K) & \to & U(L)/V(L/K) & \to & U(K) & \to & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \to & \mathrm{Gal}(M/K) & \to & U(M)/V(M/K) & \to & U(K) & \to & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

The second column is exact according to lemma (4.9). The first column is exact and so is the third row (induction hypothesis). It follows that the second row is also exact.

(4.11) Remark.

It is not difficult to extend theorem 4.3 to cover the case of nonabelian (totally ramified) galois extensions. The fundamental exact sequence then becomes

(4.11.1) $\quad 0 \to \mathrm{Gal}(L/K)^{ab} \to U(L)/V(L/K) \to U(K) \to 0$

where G^{ab} denotes the maximal abelian quotient of G. Indeed let M be the field corresponding to $\langle G,G\rangle$, the commutator subgroup of $G = \mathrm{Gal}(L/K)$. By induction on the number of elements of $\langle G,G\rangle$ we see that it suffices to prove the exactness of the sequence (4.11.1) in the case that M'/K is a sub galois extension of L/K containing M such that L/M' is abelian, and such that the fundamental sequence for M'/K is exact. We now have the following diagram.

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & \mathrm{Gal}(L/M') \arrow[r, equal] \arrow[d, "\beta"] & \mathrm{Gal}(L/M') \arrow[d] & & \\
 & \mathrm{Gal}(L/K)^{ab} \arrow[r, "i"] \arrow[d, "\alpha"] & U(L)/V(L/K) \arrow[r, "N"] \arrow[d, "\gamma"] & U(K) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathrm{Gal}(M'/K)^{ab} \arrow[r] & U(M')/V(M'/K) \arrow[r, "N"] \arrow[d] & U(K) \arrow[r] & 0 \\
 & & 0 & &
\end{tikzcd}$$

The map α is an isomorphism and β is the zero map because M' contains M, the field of invariants of $\langle G,G\rangle$. It follows that i is injective, as the bottom row is exact by induction hypothesis. The second column is exact by an argument identical with the one used in (4.9), using theorem (4,3) instead of (4,5). It follows that the second row is exact.

5. "ALMOST" THE RECIPROCITY HOMOMORPHISM

(5.1) In this section K is a local field with <u>finite</u> residue field of q elements, and L/K is a finite (abelian) galois extension which is <u>totally ramified</u>. Let K_{nr} and L_{nr} be the maximal unramified extensions of K and L and let $\hat{K}_{nr}$ and $\hat{L}_{nr}$ be their completions. The extension $\hat{L}_{nr}/\hat{K}_{nr}$ is also (abelian) galois and totally ramified and the galois group $\mathrm{Gal}(\hat{L}_{nr}/\hat{K}_{nr})$ is naturally isomorphic with $\mathrm{Gal}(L/K)$ (Cf. (2. 2)).

The algebraic closure of the residue field k of K is denoted k_s; it is the residue field of K_{nr} and $\hat{K}_{nr}$.

We use the symbol F for the Frobenius morphism of $\mathrm{Gal}(k_s/k)$ for their canonical lifts in $\mathrm{Gal}(K_{nr}/K)$ and $\mathrm{Gal}(L_{nr}/L)$ and also for their extensions to $\hat{K}_{nr}$ and $\hat{L}_{nr}$. We can now form the following diagram (cf. section 4).

(5.1.1)
$$\begin{tikzcd}
 & & X \arrow[r, "a"] \arrow[d] & Y \arrow[d] \arrow[ddddll, dashed, bend left, "g"] & \\
0 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] \arrow[d, "F-1"] & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) \arrow[r] \arrow[d, "F-1"] & U(\hat{K}_{nr}) \arrow[r] \arrow[d, "F-1"] & 0 \\
0 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] \arrow[d] & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) \arrow[r] \arrow[d] & U(\hat{K}_{nr}) \arrow[r] & 0 \\
 & C \arrow[r, "b"] & D & & \\
 & & & &
\end{tikzcd}$$

where F-1 is the homomorphism which associates $F(u)u^{-1}$ to $u \in U(\hat{K}_{nr})$; X, Y, C, D are the appropriate kernels and cokernels.

(5.2) Lemma.

(i) $F-1\colon U(\hat{K}_{nr}) \to U(\hat{K}_{nr})$ is surjective; $F-1\colon A(\hat{K}_{nr}) \to A(\hat{K}_{nr})$ is surjective.

(ii) $F-1\colon V(\hat{L}_{nr}/\hat{K}_{nr}) \to V(\hat{L}_{nr}/\hat{K}_{nr})$ is surjective.

(iii) $\mathrm{Ker}(F-1\colon U(\hat{K}_{nr}) \to U(\hat{K}_{nr})) = U(K)$.

Proof. (i) Use the filtration of $U(\hat{K}_{nr})$ by the subgroups $U^n(\hat{K}_{nr})$ of units congruent to 1 mod π_K^n. The induced homomorphisms

$$F-1\colon U(\hat{K}_{nr})/U^1(\hat{K}_{nr}) \simeq k_s^* \to k_s^* \simeq U(\hat{K}_{nr})/U^1(\hat{K}_{nr})$$

$$F-1\colon U^n(\hat{K}_{nr})/U^{n+1}(\hat{K}_{nr}) \simeq k_s \to k_s \simeq U^n(\hat{K}_{nr})/U^{n+1}(\hat{K}_{nr})$$

are

$$F-1\colon k_s^* \to k_s^*,\ x \mapsto x^{q-1}$$

$$F-1\colon k_s \to k_s,\ x \mapsto x^q - x$$

which are surjective because k_s is algebraically closed. The first part of (i) now follows by a wellknown argument concerning homomorphisms of complete filtered abelian groups. For the second part of (i) one uses the filtration by the $\pi_K^n A(\hat{K}_{nr})$ of $A(\hat{K}_{nr})$. The induced maps $F-1\colon k_s \to k_s$ are (again) the maps $x \mapsto x^q - x$.

(ii) Now let $t(x)x^{-1} \in V(\hat{L}_{nr}/\hat{K}_{nr})$. It suffices to show that these elements are in Im(F-1). Choose $y \in U(\hat{L}_{nr})$ such that $(F-1)(y) = x$. Then we have

$$(F-1)\left(\frac{t(y)}{y}\right) = \frac{Ft(y)}{F(y)} \cdot \left(\frac{t(y)}{y}\right)^{-1} = \frac{tF(y)}{t(y)} \cdot \left(\frac{F(y)}{y}\right)^{-1} = \frac{tx}{x}$$

because F and t commute as L/K is totally ramified.

(iii) Let $u \in U(\hat{K}_{nr})$, and $F(u) = u$. We write $u = u_o' + \pi_K w_1'$, with $u_o \in K_{nr}$; $F(u) = u$ yields $Fu_o' \equiv u_o' \bmod \pi_K$. Hence we can write $u = u_o + \pi_K w_1$ with $u_o \in K$; then $Fu = u$ yields $Fw_1 = w_1$.

Now write $w_1 = \pi_K^{n_1} u_1$, $u_1 \in U(\hat{K}_{nr})$; this gives $Fu_1 = u_1$; repeating this process with u_1 instead of u gives

$u = u_o + \pi_K^{n_1} u_{1o} + \pi_K^{n_1+1} w_2$, $u_o, u_{1o} \in K$. Continuing in this way we see that $u \in K \bmod \pi_K^n$ for all n, and hence that $u \in U(K)$ because K is complete.

(5.3) Definition of $\phi(L/K) : U(K) \to Gal(L/K)$.

Let L/K be totally ramified abelian. One forms the diagram (5.1.1). The rows of this diagram are exact by theorem (4.3). Therefore there is (by the snake lemma) an induced homomorphism $g : Y \to C$ as shown. According to (5.2) (iii), $Y = U(K)$. Further because L/K is totally ramified, F commutes with every $t \in Gal(L/K)$ so that $F-1$: $Gal(L/K) \to Gal(L/K)$ is the zero map, which permits us to identify C with Gal(L/K). We therefore obtain "the almost reciprocity homomorphism"

$$\phi(L/K) : U(K) \to Gal(L/K)$$

for abelian totally ramified extensions L/K.

(5.4) Proposition

(i) $\phi(L/K)$ is surjective.

(ii) $Ker(\phi(L/K)) = N_{L/K}(U(L))$.

Proof. (i) To prove (i) is suffices to show that $D = 0$ in diagram 5.1.1 which follows from the surjectivity of $F-1$: $U(\hat{L}_{nr}) \to U(\hat{L}_{nr})$ (Lemma 5.2 (i))

(ii) It is clear that $N_{L/K}(U(L)) \subset a(X)$(cf. diagram 5.1.1). Now let the element $\bar{x} \in X$ be represented by $x \in U(\hat{L}_{nr})$. Then $(Fx)x^{-1} \in V(\hat{L}_{nr}/\hat{K}_{nr})$ (because $\bar{x} \in X$). According to lemma (5.2) (ii) there is an $y \in V(\hat{L}_{nr}/\hat{K}_{nr})$ such that $(Fy)y^{-1} = (Fx)x^{-1}$. Or, in other words, $F(xy^{-1}) = xy^{-1}$, which implies $xy^{-1} \in U(L)$ by lemma (5.2) (iii). And therefore $N_{L/K}(x) = N_{L/K}(xy^{-1}) \in N_{L/K}(U(L))$; i.e. $a(\bar{x}) \in N_{L/K}(U(L))$. This concludes the proof of the proposition.

(5.5) Theorem.

For every finite abelian totally ramified extension L/K we have an isomorphism

$$\phi(L/K) : U(K)/N_{L/K}U(L) \to Gal(L/K)$$

These isomorphisms are functorial in the sense that if L/K is totally ramified abelian extension and M/K a subextension of L/K then the following diagram is commutative

$$\begin{array}{ccc} U(K)/N_{L/K}U(L) & \rightarrow & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ U(K)/N_{M/K}U(M) & \rightarrow & \mathrm{Gal}(M/K) \end{array}$$

<u>Proof</u>. The first statement is proposition 5.4. and the second statement follows from the functoriality of the connecting morphism g of the snake lemma.

(5.6) It is convenient to have a slight extension of theorem (5.5) to the case of finite abelian (not necessarily totally ramified) extensions L/K. Let F' be any lift in $\mathrm{Gal}(L_{nr}/K)$ of the Frobenius morphism in $\mathrm{Gal}(k_s/k)$; let L' be the invariant field of F. Then L'/K is abelian totally ramified and $L'_{nr} = L_{nr}$. Identifying $\mathrm{Gal}(L/K)_{ram}$ and Gal(L'/K) in the canonical way we find a diagram.

$$\begin{array}{ccccccccc} & & & & X & \xrightarrow{a} & Y & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & \mathrm{Gal}(L/K)_{ram} & \rightarrow & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) & \rightarrow & U(\hat{K}_{nr}) & \rightarrow & 0 \\ & & \downarrow F'-1 & & \downarrow F'-1 & & \downarrow F-1 & & \\ 0 & \rightarrow & \mathrm{Gal}(L/K)_{ram} & \rightarrow & U(\hat{L}_{nr})/V(\hat{L}_{nr}/\hat{K}_{nr}) & \rightarrow & U(\hat{K}_{nr}) & \rightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & C & \xrightarrow{b} & D & & & & \end{array}$$

This, as in (5.4), yields an isomorphism.

$$U(K)/N_{L'/K}(U(L')) \rightarrow \mathrm{Gal}(L/K)_{ram} = \mathrm{Gal}(L'/K)$$

But $L'.K_n = L.K_n$ for some finite unramified extension K_n/K and $L.K_n/L$ and $L'.K_n/L$ are unramified extensions. Further $N_{M'/M}(U(M')) = U(M)$ if M'/M is an unramified extension (2.3). Therefore $N_{L'/K}(U(L')) = N_{L/K}(U(L))$, which gives us an isomorphism

$$\phi(L/K) : U(K)/N_{L/K}(U(L)) \xrightarrow{\cong} \mathrm{Gal}(L/K)_{ram}$$

(5.7) <u>Theorem</u>

For every finite abelian extension L/K there is a canonical isomorphism

$$\phi(L/K)\ :\ U(K)/N_{L/K}(U(L)) \xrightarrow{\cong} \mathrm{Gal}(L/K)_{ram}$$

which is functorial in the sense that if M/K is a larger abelian extension (i.e $L \subset M$) then the following diagram commutes

$$\begin{array}{ccc} U(K)/N_{L/K}(U(L)) & \xrightarrow{\cong} & \mathrm{Gal}(L/K)_{ram} \\ \uparrow & & \uparrow \\ U(K)/N_{M/K}(U(L)) & \xrightarrow{\cong} & \mathrm{Gal}(M)/K)_{ram} \end{array}$$

where the first vertical arrow is the canonical projection and the second one is induced by the canonical projection $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$.

Proof. Cf (5.6). The functoriality follows again from the functoriality of the snake lemma.

6. THE LUBIN-TATE EXTENSIONS

As in the previous section let K be a local field with finite residue field k of q elements. Let $\pi_K = \pi$ be a uniformizing element of K; A(K) is the ring of integers of K.

(6.1) Definition of the Lubin-Tate extensions L_m/K.

Let f(X) be a polynomial over A(K) of the form

$$f(X) = X^q + \pi(a_{q-1}X^{q-1} + \dots + a_2X^2) + \pi X,\ a_2,\dots,a_{q-1} \in A(K)$$

We use $f^{(m)}(X)$ to denote the m-th iterate of f(X); i.e. $f^{(1)}(X) = f(X)$, $f^{(m)}(X) = f(f^{(m-1)}(X))$. As X divides f(X), it follows that $f^{(m-1)}(X)$ divides $f^{(m)}(X)$. For each m let λ_m be a root of $f^{(m)}(X)$ which is not a root of $f^{(m-1)}(X)$. We can choose (and shall do so) the λ_m in such a way that $f(\lambda_m) = \lambda_{m-1}$ for each $m \geq 2$. We define the Lubin-Tate extensions L_m/K as $L_m = K(\lambda_m)$.

It is the aim of this section to prove the following theorem concerning the extensions L_m/K.

(6.2) Theorem.

(i) L_m/K is totally ramified abelian. Its galois group is isomorphic to $U(K)/U^m(K)$.

(ii) $N_{L_m/K}(U(L_m)) = U^m(K)$

The proof of this is in several steps.

(6.2) Lemma. L_m/K is totally ramified; λ_m is a uniformizing element of L_m.

Proof. $f^{(m)}(X)/f^{(m-1)}(X)$ is an Eisenstein polynomial.

The second step is to show that $N_{L_m/K}(U(L_m)) \subset U^m(K)$. To do this we need a "denseness of separable polynomials" lemma.

(6.3) Lemma.

Let k be an arbitrary field, $g = X^n + a_{n-1}X^{n-1} + \ldots + a_o$ a polynomial over k such that $(n, \mathrm{char}(k)) = 1$ if $\mathrm{char}(k) \neq 0$. Then there exists an $r > 0$ and a polynomial $\tilde{g}$ of degree $\leq r-1$ such that the polynomial $h = X^r g + \tilde{g}$ is separable (i.e. has only simple roots).

Proof.

If k has infinitely many elements, we can choose $r = 1$ and g equal to some suitable constant $c \in k$. (For $\frac{d}{dX}(Xg+c)$ is independant of c and has only finitely many roots). Suppose now that $\# k = q$, then $\frac{dg}{dX} \neq 0$ (because $(n, \mathrm{char}(k)) = 1$). Let $x_1, \ldots, x_{n-1}$ be the set of roots of $\frac{dg}{dX}$. The $x_1, \ldots, x_{n-1}$ are all contained in some finite extension k' of k. Let $\# k' = q^s$, we can assume that $q^s >$ degree(g). Let h be the polynomial ($r = q^{s+1}$; $\tilde{g} := -X^q g(X) + 1$)

$$h := X^{q^{s+1}} g(X) - X^q g(X) + 1, \quad \frac{dh}{dX} = (X^{q^{s+1}} - X^q)\frac{dg}{dX}$$

If a is a root of $\frac{dh}{dX}$, then we have either that a is a root of $X^{q^{s+1}} - X^q$ and then $h(a) = 1$, or we have that a is a root of $\frac{dg}{dX}$, then $a \in k'$, hence $a^{q^s} = a$, and also $h(a) = 1$.

q.e.d.

We are now in a position to prove the inclusion $N_{L_m/K}(U(L_m)) \subset U^m(K)$.

(6.5) Theorem.

$$N_{L_m/K}(U(L_m)) \subset U^m(K)$$

Proof. Every element of $U(L_m)$ can be written as a product uu', where $u \in U^1(L_m)$ and u' a $(q-1)$-th root of unity. But

$$N(u') = (u')^{(q-1)q^{m-1}} = 1$$

where we have written N for $N_{L_m/K}$. Hence it suffices to show that $N(U^1(L_m)) \subset U^m(K)$. This is clearly true for $m = 1$, we therefore assume $m \geq 2$. Every element of $U^1(L_m)$ can be written as a sum

$$u = 1 + a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda^n + x \qquad a_i \in A(K),\ \lambda := \lambda_m,$$

with $n = m(q-1)q^{m-1} - 1$ and $v(x) \geq v(\pi^m)$, so that $(n, \mathrm{char}(k)) = 1$ ($m \geq 2$; v denotes the normalized exponential valuation on K). Consider the polynomial $d(X) = X^n + a_1X^{n-1} + \ldots + a_n$ (same a_i as in the sum above). Let g be the reduction of d to a polynomial over k. Choose r and $\tilde{g}$ as in lemma (6.4), let $\hat{g}$ be a lift of $\tilde{g}$ of the same degree as $\tilde{g}$. Let $h := X^r d + \hat{g}$. Then the reduction of h in $k[X]$ has no multiple roots, hence all roots of h are in K_{nr}. We can choose the constant term of h equal to 1, which implies that the product of the roots $z_1, \ldots, z_t$ of h is equal to ± 1, and that therefore the roots of h are all units (of K_{nr}). Then $(1-z_1\lambda)\ldots(1-z_t\lambda) = 1 + a_1\lambda + \ldots + a_n\lambda^n + x'$ with $v(x') \geq v(\pi^m)$ and $u = 1 + a_1\lambda + \ldots + a_n\lambda^n + x = (1-z_1\lambda)\ldots(1-z_t\lambda)(1+y)$ with $v(y) \geq v(\pi^m)$. Now $N(1+y) \in U^m(K)$. We have left to show that

$$N\Big(\prod_{i=1}^{t} (1-z_i\lambda)\Big) \in U^m(K)$$

It suffices to show that $N_{L_m.K_{nr}/K_{nr}}(\Pi(1-z_i\lambda))$ is in $U^m(K_{nr})$. This follows from the commutativity of the diagram below and the fact that $U^m(K_{nr}) \cap U(K) = U^m(K)$ (because K_{nr}/K is unramified).

$$(6.5.1)\qquad \begin{array}{ccc} L_m & \hookrightarrow & L_m.K_{nr} \\ \downarrow N_{L_m/K} & & \downarrow N_{L_m.K_{nr}/K_{nr}} \\ K & \hookrightarrow & K_{nr} \end{array}$$

(The commutativity **is** proved as follows. Let $x \in L_m$, then x has the same minimum polynomial over K as over K_{nr} because K_{nr}/K is unramified and L_m/K is totally ramified, q.e.d).

In particular we have that the minimum polynomial of $\lambda \in L_m.K_{nr}$ is $f^{(m)}(X)/f^{(m-1)}(X) \in K_{nr}[X]$. This yields

$$(6.5.2) \qquad N(1-z\lambda) = z^{(q-1)q^{m-1}} \frac{f^{(m)}(z^{-1})}{f^{(m-1)}(z^{-1})}, \quad z \in U(K_{nr})$$

(Thanks to the commutativity of the diagram (6.5.1) above we can and shall use N for both $N_{L_m/K}$ and $N_{L_m.K_{nr}/K_{nr}}$ indiscriminatedly).

Setting $y_i := z_i^{-1}$ we obtain from (6.5.2)

$$N\Big(\prod_{i=1}^{t} (1-z_i\lambda)\Big) = \Big(\prod_{i=1}^{t} z_i\Big)^{(q-1)q^{m-1}} \cdot \prod_{i=1}^{t} \frac{f^{(m)}(y_i)}{f^{(m-1)}(y_i)}$$

$$= \prod_{i=1}^{t} \frac{f^{(m)}(y_i)}{f^{(m-1)}(y_i)} \qquad \text{(because } \Pi z_i = \pm 1 \text{ and } m \geq 2)$$

$$= 1 + \frac{\prod_{i=1}^{t} f^{(m)}(y_i) - \prod_{i=1}^{t} f^{(m-1)}(y_i)}{\prod_{i=1}^{t} f^{(m-1)}(y_i)}$$

The z_i are units, therefore the y_i too, and also the $f^{(m-1)}(y_i)$, as is easily seen from the form of $f^{(m-1)}(X)$. It follows that it suffices to prove that

$$\prod_{i=1}^{t} f^{(m)}(y_i) - \prod_{i=1}^{t} f^{(m-1)}(y_i) \equiv 0 \bmod (\pi^m)$$

The automorphism $F \in \mathrm{Gal}(K_{nr}/K)$, the Frobenius automorphism, permutes the roots z_i of h, hence F also permutes the y_i. The homomorphism F reduces to $x \mapsto x^q \bmod (\pi)$. Therefore there exists a permutation σ of $1,\dots,t$ such that

$$f(y_i) \equiv y_{\sigma(i)} \quad \bmod (\pi)$$

because $x \mapsto f(x)$ also reduces to $x \mapsto x^q \bmod (\pi)$.

For any two elements $a, b \in A(K_{nr})$, if $a \equiv b \bmod (\pi^r)$ with $r \geq 1$ then $a^q \equiv b^q \bmod (\pi^{r+1})$ and $\pi a^s \equiv \pi b^s \bmod (\pi^{r+1})(s = 1,\dots,q-1)$ hence also $f(a) \equiv f(b) \bmod.(\pi^{r+1})$.

Applying this to the relation

$$f(y_i) \equiv y_{\sigma(i)} \mod (\pi)$$

we obtain

$$f^{(m)}(y_i) \equiv f^{(m-1)} y_{\sigma(i)} \mod (\pi^m)$$

Taking the product over i we find

$$\prod_{i=1}^{t} f^{(m)}(y_i) \equiv \prod_{i=1}^{t} f^{(m-1)}(y_{\sigma(i)}) \equiv \prod_{i=1}^{t} f^{(m-1)}(y_i) \mod (\pi^m)$$

q.e.d.

The next step (the third) consists of proving that L_m/K is galois. To do this we need the following elementary but powerfull lemma of Lubin and Tate [7].

(6.6) Lemma.

Let K be a local field with finite residue field of q elements. Let π be a fixed uniformizing element of K. Let $f(X), g(X) \in A(K)[[X]]$ be two power series over A(K) such that

$$f(X) \equiv \pi X \equiv g(X) \mod (X^2)$$

$$f(X) \equiv g(X) \equiv X^q \mod (\pi)$$

Then for every $a \in A(K)$ there exists a unique power series $[a_{f,g}](X)$ over A(K) such that

$$f([a]_{f,g}(X)) = [a]_{f,g}(g(X))$$

$$[a]_{f,g}(X) \equiv aX \mod (X^2)$$

Proof. One defines inductively polynomials $F_r(X)$ of degree r such that

$$f(F_r(X)) \equiv F_r(g(X)) \quad \mod (X^{r+1})$$

$$F_r(X) \equiv F_{r+1}(X) \quad \mod (X^{r+1})$$

One can take $F_1(X) = aX$. Suppose we have found $F_r(X)$, for a certain $r \geq 1$. One then sets $F_{r+1}(X) = F_r(X) + a_{r+1}X^{r+1}$ where a_{r+1} is yet to be determined. One has

$$f(F_{r+1}(X)) \equiv f(F_r(X)) + \pi a_{r+1} X^{r+1} \mod (X^{r+2})$$

$$F_{r+1}(g(X)) \equiv F_r(g(X)) + \pi^{r+1} a_{r+1} X^{r+1} \mod (X^{r+2})$$

These equations show that a_{r+1} must satisfy

$$a_{r+1}X^{r+1} \equiv \frac{f(F_r(X))-F_r(g(X))}{\pi^{r+1}-\pi} \qquad \mathrm{mod}(X^{r+2})$$

which proves in any case (inductively) that $F_{r+1}(X)$ is unique mod (X^{r+2}) for all r, thus taking care of the uniqueness assertion concerning $[a]_{f,g}(X)$.

It remains to show that $a_{r+1} \in A(K)$, which follows from

$$f(F_r(X)) - F_r(g(X)) \equiv (F_r(X))^q - F_r(X^q) \equiv 0 \quad \mathrm{mod}(\pi)$$

The series $[a]_{f,g}(X)$ is the limit of the F_r. This proves the lemma.

(6.7) Corollary.

(i) $[\pi]_f(X) = f(X)$

(ii) $[a]_f([b]_f(X)) = [ab]_f(X) \qquad a, b \in A(K)$

(iii) $[1]_{f,g}([1]_{g,f}(X)) = X$

Here we have written $[a]_f$ for $[a]_{f,f}$. All these equalities are proved by showing that the left and right hand side both satisfy the same characterizing properties of lemma (6.6). E.g. $[\pi]_f(X) \equiv \pi X \ \mathrm{mod}(X^2)$ and $f([\pi]_f(X)) = [\pi]_f(f(X))$; on the other hand $f(X) \equiv \pi X \ \mathrm{mod}\ (X^2)$ and $f(f(x)) = f(f(X))$. Therefore $[\pi]_f(X) = f(X)$ by the uniqueness assertion of (6.6).

Now let $f = X^q + \pi(a_{q-1}X^{q-1}+\ldots+a_2X^2) + \pi X$, as before. Taking $f = g$ in the lemma above, we have for every $u \in U(K)$ a power series $[u]_f(X)$ over A(K) such that $f[u]_f(X)) = [u]_f(f(X))$. It follows that if λ_m is a root of $f^{(m)}(X)$ which is not a root of $f^{(m-1)}(X)$, then $[u]_f(\lambda_m)$, which is in $K(\lambda_m) = L_m$ because L_m is complete and $[u]_f(X) \in A(K)[[X]]$, is another (possibly the same) root of $f^{(m)}(X)$, which is not a root of $f^{(m-1)}(X)$. To prove that L_m/K is galois it suffices to show that by varying u we get enough different roots $[u]_f(\lambda_m)$ of $f^{(m)}(X)$. A preliminary lemma for this is

(6.8) Lemma.

Let $f(X)$ be a power series over $A(K)$; let L/K be a finite extension of K and suppose that there is a $\lambda \in L$ with $v_L(\lambda) > 0$ such that $f(\lambda) = 0$. Then there exists a power series $g(X)$ over $A(L)$ such that $f(X) = (X-\lambda)g(X)$.

Proof. Write $f(X) = (X-\lambda)g_n + b_n \mod(X^n)$ with $b_n \in A(L)$ (division with remainder in $A(L)[X]$.Now $f(\lambda) = 0$, therefore $v_L(b_n) \geq nv_L(\lambda)$ which goes to infinity as $n \to \infty$ because $v_L(\lambda) > 0$. We also have $f(X) = (X-\lambda)g_{n+1}(X) + b_{n+1} \mod(X^{n+1})$. And therefore

(6.8.1) $$(X-\lambda)(g_n(X) - g_{n+1}(X)) \equiv 0 \quad \mod(\lambda^n, X^n)$$

Write

$$g_{n+1}(X) - g_n(X) = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_o$$

Using (6.8.1) one obtains

$$v_L(a_o\lambda) \geq nv_L(\lambda)$$
$$v_L(a_1\lambda - a_o) \geq nv_L(\lambda)$$

$$v_L(a_{n-1}\lambda - a_{n-2}) \geq nv_L(\lambda)$$

which implies

$$v_L(a_o) \geq (n-1)v_L(\lambda)$$
$$v_L(a_1) \geq (n-2)v_L(\lambda)$$

$$v_L(a_{n-1}) \geq 0$$

It follows that the sequence $g_n(X)$ has a limit $g(X)$ as $n \to \infty$. Then $f(X) \equiv (X-\lambda)g(X) \mod (X^n, \lambda^n)$ for all n; i.e. $f(X) = (X-\lambda)g(X)$. Which proves the lemma.

We are now in a position to prove that L_m/K is galois and to calculate its galois group.

(6.9) Proposition.

The extension L_m/K is galois; its galois group is isomorphic to $U(K)/U^m(K)$.

Proof. We first remark that if u, u' $\in$ U(K), then (cf.(6.7))

(6.9.1) $$[u]_f([u']_f(X)) = [uu']_f(X)$$

Suppose we have proved that

(6.9.2) $$[u]_f(\lambda_m) = [u']_f(\lambda_m) \Rightarrow u \equiv u' \mod(U^m(K))$$

Because $U(K)/U^m(K)$ has $(q-1)q^{m-1}$ elements and $[L_m : K] = (q-1)q^{m-1}$ it follows from (6.9.2) that L_m/K is galois. The assignment s $\in$ Gal(L_m/K) $\mapsto$ class of any u such that $s(\lambda_m) = [u]_f(\lambda_m)$ then defines an isomorphism of Gal(L_m/K) with $U(K)/U^m(K)$ (in virtue of (6.9.1)). It therefore remains to prove (6.9.2). Using (6.9.1) we see that it suffices to prove that

(6.9.3) $$[u]_f(\lambda_m) = \lambda_m \Rightarrow u \equiv 1 \mod(U^m(K))$$

Let s$\in$ G(K,L $\rightarrow$ Ω). Then $s(\lambda_m)$ is a root of $[u]_f(X) - X$, because s acts continuously. Further $f^{(r)}(\lambda_m)$ is a root of $[u]_f(X) - X$ for all $r \leq m$ because $[u]_f(f(X)) = f([u]_f(X))$. Therefore all the roots of $f^{(m)}(X)$ are roots of $[u]_f(X) - X$. Applying (6.8) repeatedly we find a factorisation

$$[u]_f(X) - X = f^{(m)}(X)g(X)$$

But $f^{(m)}(X) = \pi^m X + \ldots$. Comparing the coefficiënts of X on the left and on the right we see that

$$u - 1 = \pi^m.a$$

where a is the constant term of g(X). As g(X) has integral coefficients (cf.(6.8)) the proposition is proved.

(6.10) Corollary.

$$N_{L_m/K}(U(L_m)) = U^m(K)$$

Proof. This follows from (6.9) and theorems (5.5), (6.5).

(6.11) Remark.

The Lubin-Tate extensions L_m depend only on the choice of π , not on the choice of the polynomial $f(X) = X^q + \pi(a_{q-1}X^{q-1}+\ldots+a_2X^2) + \pi X$. Indeed, let g(X) be another polynomial of the same form. According to

Lemma (6.8) there is a unique power series $[1]_{f,g}(X)$ such that $[1]_{f,g}(X) \equiv X \bmod(X^2)$ and $f[1]_{f,g}(X)) = [1]_{f,g}(g(X))$. Now let μ_m be a root of $g^{(m)}(X)$ which is not a root of $g^{(m-1)}(X)$, then we see that $[1]_{f,g}(\mu_m)$ is a root of $f^{(m)}(X)$ which is not a root of $f^{(m-1)}(X)$ (look at $v([1]_{f,g}(\mu_m))$ for this last statement). But $[1]_{f,g}(\mu_m) \in K(\mu_m)$, and therefore $L_m \subset K(\mu_m)$ and comparing degrees we see that $L_m = K(\mu_m)$.

We can therefore talk about the Lubin-Tate extensions associated to π.

(6.12) Remark.

$\pi \in K$ is a norm from each L_m. Indeed $N_{L_m/K}(-\lambda_m) = \pi$ because the constant term of $f^{(m)}(X)/f^{(m-1)}(X)$ is equal to π, and $f^{(m)}(X)/f^{(m-1)}(X)$ is irreducible.

7. LOCAL CLASS FIELD THEORY.

In this section K is again a local field with finite residue field. Let K_{ab} be the maximal abelian extension of K. The first aim of this section is to calculate $\mathrm{Gal}(K_{ab}/K)$ and to give a description of K_{ab}. We then proceed to "extend" the "almost reciprocity homomorphism" $\phi(L/K) : U(K) \to \mathrm{Gal}(L/K)$ of §5 to a "reciprocity homomorphism" $r(L/K) : K \to \mathrm{Gal}(L/K)$ defined for all abelian L/K. And finally we give the explicit formula for r(L/K) due to Lubin and Tate (and Dwork).

(7.1) Theorem.

$$\mathrm{Gal}(K_{ab}/K)_{ram} \simeq U(K) \; ; \; \mathrm{Gal}(K_{ab}/K) \simeq U(K) \times \hat{Z}$$

Proof. For every finite abelian extension L/K we have an isomorphism

(7.1.1) $$\phi(L/K): U(K)/N_{L/K}(U(L)) \to \mathrm{Gal}(L/K)_{ram}$$

Taking the limit over all finite abelian L/K we obtain an isomorphism

(7.1.2) $$\phi : \varprojlim U(K)/N_{L/K}(U(L)) \xrightarrow{\sim} \mathrm{Gal}(K^{ab}/K)_{ram}$$

(cf. §3.) Now U(L) is compact and $N_{L/K}$ is continuous. It follows that $N_{L/K}(U(L))$ is compact and therefore closed in U(K). As it is also a subgroup of finite index (by (5.7)), it is also open in $U(K)$; i.e. there exists an n (depending on L) such that $N_{L/K}(U(L)) \supset U^n(K)$. By theorem (6.2) there exists for every $m \in N$ an abelian extension L_m/K such that $N_{L_m/K}(U(L_m)) = U^m(K)$. It follows from these facts that the projective limit on the left of 7.12 is equal to $U(K)$. This proves the first part of the theorem and also the second in virtue of (3.4).

Fix a uniformizing element π of K. Let L_m be the Lubin-Tate extensions corresponding to this choice of π. (Cf. (6.1) and (6.11)).

We write $L_\pi = \bigcup_m L_m$.

7.2. <u>Corollary</u> $K_{ab} = L_\pi . K_{nr}$

<u>Proof</u>. $L_\pi . K_{nr}$ is an abelian extension and therefore contained in K_{ab}.

We have a commutative diagram with exact rows.

$$\begin{tikzcd}
 & 0 \arrow[r] & \mathrm{Gal}(K_{ab}/K)_{ram} \arrow[r] \arrow[dd, "\alpha'"] & \mathrm{Gal}(K_{ab}/K) \arrow[r] \arrow[dd, "\alpha"] & \mathrm{Gal}(K_{nr}/K) \arrow[r] \arrow[dd, equal] & 0 \\
U(K) \arrow[urr, "\phi(K_{ab}/K)"] \arrow[drr, "\phi(L_\pi . K_{nr}/K)"'] & & & & & \\
 & 0 \arrow[r] & \mathrm{Gal}(L_\pi . K_{nr}/K)_{ram} \arrow[r] & \mathrm{Gal}(L_\pi . K_{nr}/K) \arrow[r] & \mathrm{Gal}(K_{nr}/K) \arrow[r] & 0
\end{tikzcd}$$

where α is the natural projection, α' is induced by α, and the homomorphisms $\phi(K_{ab}/K)$ and $\phi(L_\pi . K_{nr}/K)$ are obtained by taking the projective limit of the homomorphisms $\phi(L/K)$ where L/K runs through the abelian subextensions of K_{ab} and $L_\pi . K_{nr}$ respectively.

Now $\phi(L_\pi . K_{nr}/K)$ is the projective limit of the isomorphisms $\phi(L_m/K) : U(K)/N_{L_m/K}(U(L_m)) \xrightarrow{\sim} \mathrm{Gal}(L_m/K)$ and as $N_{L_m/K}(U(L_m)) = U^m(K)$ by theorem (6.2) we conclude that $\phi(L_\pi . K_{nr}/K)$ is an isomorphism. The homomorphism $\phi(K_{ab}/K)$ is also an isomorphism (Theorem 7.1) and therefore α' is an isomorphism and thus α too, which concludes the proof of the corollary.

(7.3) The group $U(K) \times \hat{Z}$ is the completion of $K^* \simeq U(K) \times Z$ with respect to the topology of open subgroups of finite index. (Open in the sense of the topology on K^* induced by the valuation on K). When regarded as this completion we shall write $\tilde{K}^*$ for $U(K) \times \hat{Z}$ and $K^* \to \tilde{K}^*$ will be the natural inclusion.

One can of course choose many isomorphisms $\tilde{K}^* \simeq U(K) \times \hat{Z} \simeq \mathrm{Gal}(K^{ab}/K)$.

It is the aim of the next few subsections to show that we can choose this isomorphism in such a way that the kernel of

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

is precisely $N_{L/K}(L^*) \subset K^*$ for every abelian L/K (where the last map is the natural projection).

(7.4) <u>Preliminary definition</u>.

Let L'/K be a totally ramified abelian extension; π_K a uniformizing element of K which is a norm from L'; and K_n/K an unramified (abelian) extension of K. We define a homomorphism $r\colon K^* \to \mathrm{Gal}(L'.K_n/K)$ as follows. (We should of course write $r_{L'.K_n}$ or something similar).

$$U(K) \ni u \mapsto r(u) := \phi(u^{-1}) \in \mathrm{Gal}(L'/K) = \mathrm{Gal}(L'.K_n/K_n) = \mathrm{Gal}(L'.K_n/K)_{ram}$$

$$\pi_K \mapsto F \in \mathrm{Gal}(L'.K_n/L')$$

where F is the Frobenius automorphism of $\mathrm{Gal}(L'.K_n/L')$ and $u \mapsto \phi(u)$ is the homomorphism defined in (5.5).

The first step now is to show that this definition does not depend on the choice of L' in $L'.K_n$, and to show that for this definition one does have the kernel property mentioned in 7.3. To this end we need the following lemma, which is also usefull further on

(7.5) <u>Lemma</u>.

Let L/K be an abelian extension. The index of $N_{L/K}(L^*)$ in K is equal to the number $\# \mathrm{Gal}(L/K)$.

<u>Proof</u>. Let K_L be the maximal unramified extension of K contained in L. We have $[L : K_L] = \#(U(K)/N_{L/K}(U(L)))$ (cf. (5.7)). There is an exact diagram.

$$\begin{tikzcd}
0 \arrow[r] & U(L) \arrow[r] \arrow[d, "N_{L/K}"] & L^* \arrow[r, "v_L"] \arrow[d, "N_{L/K}"] & \mathbb{Z} \arrow[r] \arrow[d, "\times f_{L/K}"] & 0 \\
0 \arrow[r] & U(K) \arrow[r] & K^* \arrow[r, "v_K"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where $f_{L/K} := [K_L : K]$. Hence $\#(K^*/N_{L/K}(L^*)) = \#(U(K)/N_{L/K}(U(L))).f_{L/K} =$
$= [L:K_L][K_L:K] = \#\ \mathrm{Gal}(L/K)$.

q.e.d.

(7.6) Lemma.

Let $L'' \subset L'.K_n$ be any other totally ramified abelian extension such that $L''.K_n = L'.K_n$ (i.e. $[L':K] = [L'':K]$; same situation as in the definition of r above). Then

$$\mathrm{Ker}(K^* \xrightarrow{r} \mathrm{Gal}(L'.K_n/K) \to \mathrm{Gal}(L''/K)) = N_{L''/K}(L''^*).$$

Proof. Lemma (7.5) implies that it suffices to show that $N_{L''/K}(L''^*) \subset \mathrm{Ker}(..)$

For this it suffices to show that $N_{L''/K}(\pi'') \in \mathrm{Ker}(...)$ when π'' is a uniformizing element of L'' (Because $N_{L''/K}(U(L'')) \subset \mathrm{Ker}(r)$ because of (5.7) or because the uniformizing elements of L''

generate L''^*). Let L'' be the invariant field of $r(u)F$. Such an $u \in U(K)$ exists because $r(U(K)) = \mathrm{Gal}(L'.K_n/K)_{ram}$. Cf. (5.7). Write $\pi'' = x\pi'$ where $\pi' \in L'$ is such that $N_{L'/K}(\pi') = \pi_K$. We have

$$\pi_K = N_{L'.K_n/K_n}(\pi') = N_{L'.K_n/K_n}(x^{-1}).N_{L'.K_n/K_n}(\pi'') =$$

$$= N_{L'.K_n/K_n}(x^{-1}).N_{L''/K}(\pi'')$$

It follows that

(7.6.1) $$N_{L'.K_n/K_n}(x) \in U(K)$$

Now $r(u)F(\pi'') = \pi''$. Therefore using $F(\pi') = \pi'$ and $x\pi' = \pi''$ we have in the group $U(\hat{L}'_{nr}) = U(\hat{L}''_{nr})$

(7.6.2) $$\frac{\phi(u^{-1})(\pi')}{\pi'} = \frac{r(u)(\pi')}{\pi'} = \frac{r(u)F(\pi')}{\pi'} = \frac{r(u)F(x^{-1})}{x^{-1}} =$$

$$= \frac{r(u)F(x^{-1})}{F(x^{-1})} \cdot \frac{F(x^{-1})}{x^{-1}} \equiv \frac{F(x^{-1})}{x^{-1}} \bmod V(\hat{L}'_{nr}/\hat{K}_{nr})$$

Hence by the definition of the isomorphism ϕ in (5.5) we must have (in virtue of (7.6.1) and (7.6.2))

(7.6.3) $$N_{L'.K_n/K_n}(x) \equiv u \mod N_{L'/K}(U(L'))$$

and hence

$$r(N_{L''/K}(\pi'')) = r(u\pi_K) = r(u)F$$

which is the identity on L". This proves the lemma

(7.7) Corollary.

The definition of r in (7.4) is independant of the choice of L'. More precisely if we had used an L" as in (7.6) instead of L'for the definition of r; i.e. if we had defined

$$U(K) \ni u \to (r(u) = \phi(u^{-1})$$

$$N_{L''/K}(\pi'') \to F'$$

where F' is the Frobenius automorphism of $Gal(L''.K_n/L'')$, then we would have obtained the same homomorphism r.

(7.8) Definition of the reciprocity homomorphism.

Choose a uniformizing element π of K. Let L_π be as before (cf.(7.1)) then $K_{ab} = L_\pi.K_{nr}$ (7.2). Now define

$$r : K^* \to Gal(K_{ab}/K)$$

$$U(K) \ni u \mapsto r(u) = \phi(u^{-1}) \in Gal(L_\pi/K) = Gal(K_{ab}/K_{nr})$$

$$\pi \mapsto F \in Gal(K_{ab}/L_\pi)$$

(7.9) Remarks.

There are several remarks to be made concerning this definition.

1. As π is in $N_{L_m/K}(L_m^*)$ for all m, cf.(6.12), this definition agrees with the one given in (7.4).
2. This definition is independant of the choice of π. (By (7.7) and (7.9) Remark 1
3. The homomorphism r is determined by its values on the uniformizing elements of K.
4. The homomorphism r is the restriction to K* of an isomorphism $\tilde{K}^* \to Gal(K^{ab}/K)$. Cf. (7.3)

(7.10) Theorem.

Let L/K be an abelian extension, then we have

$$\mathrm{Ker}(K^* \to \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K) = N_{L/K}L^*)$$

Proof. It suffices to prove that $N_{L/K}(L^*)$ is contained in this kernel (7.5). Let K_n be the maximal unramified extension of K contained in L; let $[K_n : K] = n$. Let r_n be the reciprocity homomorphism for the base field K_n. Then we claim that the following diagram is commutative.

$$\begin{tikzcd} K_n^* \arrow[r, "N_{K_n/K}"] \arrow[d, "r_n"] & K^* \arrow[d, "r"] \\ \mathrm{Gal}(L/K_n) \arrow[r] & G(L/K) \end{tikzcd} \qquad (7.10.1)$$

To see this, let L'/K be a totally ramified abelian extension such that $L'.K_m = L.K_m$ for some unramified extension K_m/K of degree m.We can assume that $K_n \subset K_m$. We have the following diagram of field extensions

$$\begin{tikzcd} & L \arrow[rr, dash] \arrow[d, dash] & & L'.K_m = L.K_m \\ L' \arrow[r, dash] \arrow[d, dash] & K_n \arrow[r, dash] & L'.K_n \arrow[r, dash] & L'.K_m = L.K_m \arrow[d, dash] \\ K \arrow[r, dash] & K_n \arrow[rr, dash] & & K_m \end{tikzcd}$$

Let $F \in \mathrm{Gal}(L'.K_m/L')$ be the Frobenius automorphism. Then F^n is the Frobenius automorphism of $L'.K_m/L'.K_n$. Let π be a uniformizing element of K which is in $N_{L'/K}(L'^*)$. Then (cf. (7.4))

$$(7.10.2) \qquad r_n(\pi) = F^n,\ r(N_{K_n/K}(\pi)) = r(\pi^n) = F^n$$

It remains to check that

$$(7.10.3) \qquad r_n(u) = r(N_{K_n/K}(u)) \text{ for } u \in U(K_n)$$

To this end let $u' \in U(\hat{L}'_{nr}) = U(\hat{L}_{nr})$ be a lift of u (for the norm map

$\hat{U}(L_{nr} \to U(\hat{K}_{nr}))$. The element $u'' = u'.Fu',\ldots, F^{n-1}u'$ is then a lift of $N_{K_n/K}(u) = u.Fu, \ldots, F^{n-1}u$. The element

$r_n(u) \in \mathrm{Gal}(L'.K_m/K_m) = \mathrm{Gal}(L'.K_n/K_n)$ is according to (5.5) and (7.4) characterized by

$$\frac{r_n(u)(\pi_{L'})}{\pi_{L'}} \equiv \frac{u'}{F^n u'} \mod V(\hat{L}_{nr}/\hat{K}_{nr})$$

where $\pi_{L'}$ is any uniformizing element of L'. Hence

$$\frac{r_n(u)\pi_{L'}}{\pi_{L'}} \equiv \frac{u'.Fu'.\ldots.F^{n-1}u}{Fu'.F^2u'\ldots F^n u'} = \frac{u''}{Fu''} \mod V(\hat{L}'_{nr}/\hat{K}_{nr})$$

But $r(v) \in \mathrm{Gal}(L'.K_m/K_m)$ for $v \in U(K)$ is characterized by

$$\frac{r(v)\pi_{L'}}{\pi_{L'}} \equiv \frac{v'}{Fv'} \mod V(\hat{L}_{nr}/\hat{K}_{nr})$$

where v' is any lift of v. It follows that

$$(7.10.4) \qquad r_n(u) = r(N_{K_n/K}(u)) \in \mathrm{Gal}(L'.K_m/K_m) \subset \mathrm{Gal}(L'.K_m/K_n).$$

Taking account of (7.10.2) we have shown that the diagram

$$(7.10.5) \qquad \begin{array}{ccc} K_n^* & \xrightarrow{N_{K_n/K}} & K \\ \downarrow r_n & & \downarrow r \\ \mathrm{Gal}(L'.K_m/K_n) & \to & \mathrm{Gal}(L'.K_m/K) \end{array}$$

is commutative , which implies the commutativity of (7.10.1). The kernel of r_n in (7.10.1) is equal to $N_{L/K_n}(L^*)$ according to (7.6). It follows that

$$N_{L/K}(L^*) = N_{K_n/K}(N_{L/K_n}(L^*)) = N_{K_n/K}(\mathrm{Ker}\ r_n) \subset \mathrm{Ker}\ r.$$

(cf. (7.10.1)). This proves the theorem.

(7.11) Corollary.

The norm subgroups of K^* (i.e. the subgroups $N_{L/K}(L^*)$ where L/K is an (abelian) finite extension of K) are precisely the open subgroups of finite index.

For every open subgroup R of finite index in K there is one abelian extension L/K such that the kernel of $r : K^* \to Gal(K_{ab}/K) \to Gal(L/K)$ is precisely R.

Proof. A norm subgroup is necessarily open of finite index. The rest of the corollary follows from (7.10) and the fact that $r : K^* \to Gal(K_{ab}/K)$ is the restriction to K^* of an isomorphism $\tilde{K}^* \simeq Gal(K_{ab}/K)$.

The last part of this section is devoted to the explicit determination of the reciprocity homomorphism r à la Lubin-Tate. The main tool is

(7.12) Lemma ([7] Lemma 2)

Let π and π' be two uniformizing elements of K, and let f(X),g(X) be polynomials of degree q such that $f(X) \equiv g(X) \equiv X^q \bmod \pi$ and $f(X) \equiv \pi X \bmod (X^2)$, $g(x) \equiv \pi' X \bmod X^2$. Let $\pi' = u\pi$. Then there exists a formal series $\vartheta(X) \in A(\hat{K}_{nr})[[X]]$ such that

(7.12.1) $\vartheta^F(X)) = \vartheta([u]_f(X))$, $\vartheta(X) \equiv \varepsilon X \bmod (X^2)$, for a certain $\varepsilon \in U(\hat{K}_{nr})$.

where F is the Frobenius automorphism in $Gal(K_{nr}/K)$ and also its extension to $\hat{K}_{nr}$, and $\vartheta^F(X))$ is the series obtained from $\vartheta(X)$ by letting F act on the coefficients of (X).

Proof. Because $F-1 : U(\hat{K}_{nr}) \to U(\hat{K}_{nr})$ is surjective there is an $\varepsilon \in U(\hat{K}_{nr})$ such that $u = F(\varepsilon)\varepsilon^{-1}$. Define $\vartheta_1(X) = \varepsilon X$, then $\vartheta_1^F(X) \equiv \vartheta_1([u]_f(X)) \bmod (X^2)$.

Now suppose we have already found $\vartheta_r(X)$ such that

(7.12.2) $$\vartheta_r^F(X) \equiv \vartheta_r([u]_f(X)) \mod (X^{r+1})$$

we define $\vartheta_{r+1}(X) = \vartheta_r(X) + b_{r+1}X^{r+1}$, where $b_r \in A(\hat{K}_{nr})$ is yet to be determined. Now

$$\vartheta^F_{r+1}(X) \equiv \vartheta^F_r(X) + F(b_{r+1})X^{r+1} \quad \mathrm{mod}(X^{r+2})$$

(7.12.3) $$\vartheta_{r+1}([u]_f(X)) \equiv \vartheta_r([u]_f(X)) + b_{r+1}u^{r+1}X^{r+1} \quad \mathrm{mod}(X^{r+2})$$

Let

(7.12.4) $$\vartheta^F_r(X) - \vartheta_r([u]_f(X)) \equiv -cX^{r+1} \quad \mathrm{mod}(X^{r+2})$$

Then we must choose b_{r+1} such that $F(b_{r+1}) = c + b_{r+1}u^{r+1}$. Writing $b_{r+1} = a_{r+1}\varepsilon^{r+1}$, a_{r+1} must satisfy (use $F(\varepsilon) = \varepsilon u$)

(7.12.5) $$F(a_{r+1}) - a_{r+1} = (\varepsilon u)^{-(r+1)}c$$

Such an a_{r+1} exists because $F-1\colon A(\hat{K}_{nr}) \to A(\hat{K}_{nr})$ is surjective (cf. Lemma (5.2)). Let $\vartheta(X) = \lim \vartheta_r(X)$. This proves the lemma.

7.13) <u>Corollary</u> ([7] Lemma 2)

Under the conditions of lemma (7.12) there exists a $\vartheta(X) \in A(\hat{K}_{nr})[[X]]$ such that (7.12.1) holds and moreover

(7.13.1) $$\vartheta([a]_f(X)) = [a]_g(\vartheta(X)) \quad \text{for all } a \in A(K)$$

<u>Proof</u>. We first remark that $[\pi]_f(X) = f(X)$ and $[\pi']_g(X) = g(X)$. Cf.(6.7) (i)

Let $\vartheta(X)$ be as in (7.12). We consider

(7.13.2) $$h(X) = \vartheta^F(f(\vartheta^{-1}(X)) = \vartheta([u]_f(f(\vartheta^{-1}(X)))) = \vartheta([\pi']_f(\vartheta^{-1}(X))),$$

where $\vartheta^{-1}(X)$ is defined by $\vartheta(\vartheta^{-1}(X)) = X = \vartheta^{-1}(\vartheta(X))$. (One uses (6.7) (i) and (6.7) (ii) to obtain the last equality). The series $h(X)$ has its coefficients in $A(K)$ because

$$h^F(X) = \vartheta^F(([\pi']_f)^F((\vartheta^{-1})^F(X))) = \vartheta^F(f([u]_f((\vartheta^{-1})^F(X)) =$$
$$= \vartheta^F(f(\vartheta^{-1}(X))) = h(X)$$

(for the one but last equality substitute $(\vartheta^{-1})^F(X)$ for X in (7.12.1). Further

$$h(X) \equiv F(\varepsilon)\pi\varepsilon^{-1}X \equiv u\pi X \equiv \pi' X \quad \mathrm{mod}(X^2)$$

and

$$h(X) \equiv \vartheta^F(f(\vartheta^{-1}(X))) \equiv \vartheta^F((\vartheta^{-1}(X))^q \equiv \vartheta^F((\vartheta^{-1})^F(X^q)) \equiv X^q \quad \mathrm{mod}(\pi)$$

Therefore $h(X)$ is a power series of the type considered in (6.6). And there exists therefore a unique power series $[1]_{g,h}(X)$ such that $[1]_{g,h}(X) \equiv X \bmod (X^2)$ and $g([1]_{g,h}(X)) = [1]_{g,h}(h(X))$. Now let

(7.13.3) $$\vartheta'(X) = [1]_{g,h}(\vartheta(X))$$

then (7.12.1) also holds for ϑ' (because $[1]_{g,h}(X)$ has its coefficients in $A(K)$. Consider the series

$$\ell(X) = \vartheta'([a]_f((\vartheta')^{-1}(X)))$$

We have

$$g(\ell(X)) = g([1]_{g,h}(\vartheta([a]_f(\vartheta^{-1}([1]_{h,g}(X)))))) =$$

$$= [1]_{g,h}(h(\vartheta[a]_f(\ ^{-1}([1]_{h,g}(X)))))) =$$

$$= [1]_{g,h}(\vartheta([\pi']_f([a]_f(\vartheta^{-1}([1]_{h,g}(x)))))) =$$

$$= [1]_{g,h}(\vartheta([a]_f([\pi']_f(\vartheta^{-1}([1]_{h,g}(X)))))) =$$

$$= [1]_{g,h}(\vartheta([a]_f(\vartheta^{-1}(h)([1]_{h,g}(X))))) =$$

$$= [1]_{g,h}(\vartheta([a]_f(\vartheta^{-1}([1]_{h,g}(g(X)))))) =$$

$$= \ell(g(X))$$

where we have used $h(X) = \vartheta([\pi']_f(\vartheta^{-1}(X)))$ twice and $[1]^{-1}_{g,h}(X) = [1]_{h,g}(X)$ and $[\pi']_f([a]_f(X)) = [\pi'a]_f(X) = [a]_f([\pi']_f(X))$. Cf. (6.7)

Thus $\ell(X)$ satisfies the conditions which define $[a]_g(X)$ so that (6.6) $\ell(X) = [a]_g(X)$, which proves the corollary.

(7.14) Definition.

We now define a homomorphism $s_\pi : K^* \to \mathrm{Gal}(L_\pi . K_{nr}/K)$ as follows

$s_\pi(\pi) = F \in \mathrm{Gal}(L_\pi.K_{nr}/L_\pi)$ (The Frobenius automorphism)

$s_\pi(u) = [u^{-1}]_f \in \mathrm{Gal}(L_\pi.K_{nr}/K_{nr})$ for $u \in U(K)$

where $[u^{-1}]_f$ is the automorphism of $\mathrm{Gal}(L_\pi.K_{nr}/K_{nr}) = \mathrm{Gal}(L_\pi/K)$ which acts on the λ_m as $\lambda_m \mapsto [u^{-1}]_f(\lambda_m)$. (i.e. substitute λ_m in the series $[u^{-1}]_f(X)$).

(7.15) Theorem ([6] theorem 3 and its corollary)

The homomorphism s_π is independent of π and coincides with the reciprocity homomorphism r defined in (7.8).

Proof. We first show that $s_\pi(\pi') = s_{\pi'}(\pi')$, for all uniformizing elements $\pi, \pi' \in K$. This suffices to prove the first part of the theorem. Now on $K_{nr} \subset K_{nr}.L_\pi = K_{ab} = K_{nr}.L_{\pi'}$ both $s_\pi(\pi')$ end $s_{\pi'}(\pi')$ induce the Frobenius automorphism. On $L_{\pi'}$, $s_{\pi'}(\pi')$ is the identity Thus it suffices to show that $s_\pi(\pi')$ is the identity on $L_{\pi'}$; i.e. we have to show that

$$s_\pi(\pi')(\lambda'_m) = \lambda'_m$$

for all m, where λ'_m is a root of $g^{(m)}(X)/g^{(m-1)}(X)$ where $g(X)$ is a monic polynomial of degree q such that $g(X) \equiv X^q \bmod \pi'$ and $g(X) \equiv \pi' X \bmod (X^2)$.

Let $\vartheta(X)$ be a power series over $A(\hat{K}_{nr})$ such that (7.12.1) and (7.13.1) hold. Then because $[\pi]_f(X) = f(X)$ and $[\pi']_g = g(X)$ we have because of (7.13.1) that $\vartheta(\lambda_m)$ is a root of $g^m(X)/g^{(m-1)}(X)$.

Now $s_\pi(\pi') = s_\pi(u)s_\pi(\pi) = s_\pi(u).F$, where F is the Frobenius automorphism in $\mathrm{Gal}(L_\pi.K_{nr}/L_\pi) \subset \mathrm{Gal}(K_{ab}/K)$. Thus

$$\begin{aligned} s_\pi(\pi')(\lambda'_m) &= s_\pi(u).F(\vartheta(\lambda_m)) = \\ &= s_\pi(u)(\vartheta([u]_f(\lambda_m))) = \\ &= \vartheta([u]_f(s_\pi(u)(\lambda_m))) \\ &= \vartheta([u]_f([u^{-1}]_f(\lambda_m))) \\ &= \vartheta(\lambda_m) = \lambda'_m . \end{aligned}$$

The second assertion of the theorem now follows easily because for every uniformizing element $\pi \in K$ both $r(\pi)$ and $s_\pi(\pi)$ are the Frobenius on K_{nr} and the identity on L_π.

q.e.d.

8. CONCLUDING REMARKS

In this section we add a few extra comments to the foregoing.

(8.1) "Almost the reciprocity morphism" for arbitrary finite galois extensions L/K.

Let L/K be any finite galois extension. Then the diagram of 5.1 (or rather, a similar diagram), gives an isomorphism

$$U(K)/N_{L/K}(U(L)) \to Gal(L/K)_{ram}/\langle Gal(L/K)_{ram}, Gal(L/K)\rangle$$

(8.2) Functoriality of the reciprocity homomorphism

Let $r_K : K^* \to Gal(K_{ab}/K)$ be the reciprocity homomorphism for the base field K. Then if L/K is a finite galois extension of K, the following diagram is commutative

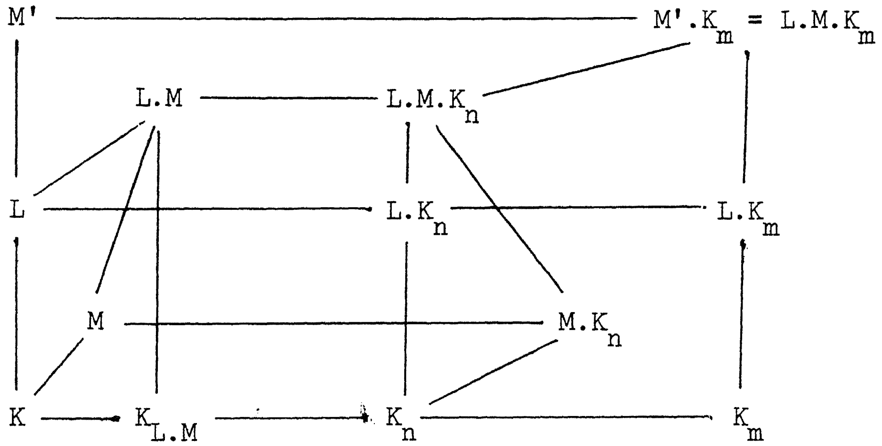
(8.2.1)
$$\begin{array}{ccc} L^* & \xrightarrow{N_{L/K}} & K^* \\ \downarrow r_L & & \downarrow r_K \\ Gal(L_{ab}/L) \xrightarrow{a} & Gal(K_{ab}.L/L) & \xrightarrow{b} Gal(K_{ab}/K) \end{array}$$

where a is the natural projection and b is the restricting of automorphisms of $K_{ab}.L$ to K_{ab}.

In the case of an unramified extension L/K this has already been proved (commutativity of diagram (7.10.5). It thus suffices to prove the commutativity of (8.2.1) in the case that L/K is a totally ramified abelian extension.

We have to show that $a \circ r_L = r_K N_{L/K}$. I.e. we only have to worry about abelian extensions of L "arising from some subextension of K_{ab}/K."

Let M/K be a totally ramified abelian extension and K_n/K an unramified extension of K. The extension $L.M/K$ is abelian. By enlarging K_n if necessary we can assume that the maximal unramified subextension of $L.M$ is contained in K_n. By means of a similar argument as in §3 we find an abelian extension M'/K such that M' contains L and such that $M'.K_m = L.M.K_m$ for some unramified extension K_m which contains K_n.



We can now use M'/L and $L.K_m/L$ to define $r_L : L^* \to Gal(M'.K_m/L)$ and M'/K and K_m/K to define $r_K : K^* \to Gal(M'.K_m/K)$.

Let $u \in U(L)$ and $u' \in U(M'_{nr})$ a lift of u for $N_{\hat{M}'_{nr}/\hat{L}_{nr}} : U(\hat{M}'_{nr}) \to U(\hat{L}_{nr})$.

Then u' is also a lift of $N_{L/K}(u)$ for $N_{\hat{M}'_{nr}/\hat{K}_{nr}} : U(\hat{M}'_{nr}) \to U(\hat{K}_{nr})$,

which proves that $r_L(u) = r_K(N_{L/K}(u))$ for $u \in U(L)$, in view of the definition of $r_L(u)$. Cf. §5 and (7.4).

And if π' is a uniformizing element of M', we have that

$r_L(N_{M'/L}(\pi')) = F \in Gal(M'.K_m/M') = Gal(M'.L.K_m/M')$ and

$r_K(N_{M'/K}(\pi')) = F \in Gal(K_m.M'/M')$

q.e.d.

(8.3) Ramification.

Keeping track of ramification in the fundamental exact sequence and the diagram 5.1.1 one sees that $\phi(L/K)$ and hence also r is ramification preserving, in the sense that $r_K : K^* \to Gal(L/K)$ maps

$U^i(K)$ into $Gal^i(L/K)$, where $Gal^i(L/K)$ is the i-th ramification subgroup of $Gal(L/K)$ (upper numbering).

(8.4) <u>The case</u> $K = Q_p$

In the case $K = Q_p$, taking $\pi = p$, $f(X) = (X+1)^p - 1$, one finds $f^{(m)}(X) = (1+X)^{p^m} - 1$. The elements of λ_m then are of the form $\zeta_m - 1$, where ζ_m is a primitive p^m-th root of unity. In this case one has $[u]_f(X) = (1+X)^u - 1$ for each p-adic integer u. Hence $[u]_f(\zeta_m - 1) = \zeta_m^u - 1$ and the formula (7.14) becomes the explicit cyclotomic reciprocity formula given by Dwork in [1] .

REFERENCES

[1]. B. Dwork (1958), Norm Residue Symbol in Local Number Fields. Abh. Math. Sem. Hamburg <u>22</u>, 180-190.

[2]. M. Hall, Jr. (1959), Theory of Groups. MacMillan.

[3]. H. Hasse (1967), Vorlesungen über Klassenkörpertheorie. Physica Verlag, Würzburg.

[4]. M. Hazewinkel (1969), Maximal Abelian Extensions of Local Fields. Thesis, Amsterdam.

[5]. M. Hazewinkel (1970), Corps de Classes Local. Appendice dans M. Demazure, P. Gabriel. Groupes Algébriques, tome 1, North Holland.

[6]. S. Lang, Algebraic Groups over Finite Fields. Am. J. Math.

[7]. J. Lubin, J. Tate (1965), Formal Complex Multiplication in Local Fields. Ann. Math. <u>81</u>, 380-387.

[8]. J.P. Serre (1962), Corps Locaux, Hermann.

[9]. E. Weiss (1963), Algebraic Number Theory. McGraw-Hill.