ABELIAN EXTENSIONS OF LOCAL FIELDS

M. Hazewinkel

STELLINGEN

1. Als twee algebraische groepen schema's G en G′ over een perfect lichaam k quasi-algebraisch equivalent zijn, dan geldt:

$$\mathrm{Ext}(G,S_k) \simeq \mathrm{Ext}(G',S_k)$$

voor elk constant algebraisch groepenschema S_k. Dit maakt het mogelijk de stelling (5.4.D) uit dit proefschrift te bewijzen zonder quasi-algebraische groepen in te voeren.

M. Hazewinkel. Crops de classes local. Appendix in: M. Demazure, P. Gabriel. Groupes Algebriques. North Holland Publ. Cy., verschijnt binnenkort.

2. Zij K een lokaal lichaam met perfect restklassen lichaam k; zij L een eindige separabele uitbreiding van K met restklassenlichaam l. Laat U_L het pro-algebraisch groepenschema over l van eenheden van L zijn. Als er een onvertakte uitbreiding K_n/K is zodat $L.K_n/K_n$ galois is, dan bestaat er een pro-algebraisch groepenschema U over k zodat $(U)_l \simeq U_L$.

3. Zij K een lokaal lichaam met een eindig restklassen lichaam, bestaande uit q elementen; laat A(K) de ring van gehelen van K zijn en π een uniformiserende. $\mathfrak{F}_\pi = \{f \in A(K)[[X]] \mid f \equiv \pi X \bmod X^2,\ f \equiv X^q \bmod \pi\}$ Zij $f^{(m)}$ de m^e geïtereerde van f; λ een wortel van $f^{(m)}$, dan is $K(\lambda)$ een totaal vertakte abelse uitbreiding van K (cf. §11 van dit proefschrift). Omgekeerd geldt: voor elke uniformiserende λ' van $K(\lambda)$ is er een $g \in \mathfrak{F}_\pi$ zodat $g^{(m)}(\lambda') = 0$.

4. Zij G een eindige groep; A een G-moduul zodat ${}_pA = \{a \in A \mid pa = 0\}$ eindig is voor alle priemgetallen p (die #G delen). Stel dat de groepen $H^q(G,A)$ en $H^{q+1}(G,A)$ eindig zijn voor een zekere $q \in \mathbf{Z}$, dan is $H^n(G,A)$ eindig voor alle $n \in \mathbf{Z}$.

5. Zij B^n de n-dimensionale bal; ∂B^n zijn rand.
   a) Als $f: B^n \to B^n$ een differentieerbare afbeelding is zodat $f|\partial B^n = \mathrm{id}$., dan is er een inwendig dekpunt van f in de gevallen:
      1° $\det(df) > 1$ op ∂B^n;
      2° $\det(df) < 1$ op ∂B^n en f is injectief.
   b) Zij $f: B^n \to B^n$ een continue functie zonder inwendige dekpunten zodat $f|\partial B^n = \mathrm{id}$.. Dan is er voor elke $\alpha > 0$ en elke P in het inwendige van B^n een punt x op afstand $< \epsilon$ van ∂B^n, zodat de lijn door x en f(x) door P gaat.

6. Zij $0 < \lambda_1 < \lambda_2 < \ldots < \lambda_n$, $P_i \in \mathbf{R}$, $i = 1,\ldots,n$, zodat $\sum_{i=1}^{k} P_i > 0$ voor alle $k = 1,\ldots,n$. Stel dat $\mu_1,\ldots,\mu_{n-1}$ de $(n-1)$ nulpunten zijn van de functie

$$f(z) = \sum_{i=1}^{n} \frac{Pk}{z-\lambda_k} .$$

Dan geldt $\sigma_i(\lambda_1,\ldots,\lambda_{n-1}) < \sigma_i(\mu_1,\ldots,\mu_{n-1})$ waarbij $\sigma_1,\ldots,\sigma_{n-1}$ de eerste $(n-1)$ elementair symmetrische functies zijn.

7. Een algebra $A = k[X]/(f)$ is dan en slechts dan star (rigid) als de tweede Hochschild cohomologie groep $H^2(A,A) = 0$. Dit is dan en slechts dan het geval als alle nulpunten van f in een algebraïsche afsluiting $\bar{k}$ van k geïsoleerd liggen.

A. Nijenhuis. Graded Lie Algebras and their applications. Univ. of A'dam 1963/1964. Lecture notes.

8. Zij **C** een kleine categorie; Λ de functor die aan een object $X \in \mathbf{C}$ de verzameling van zeven boven X toevoegt. Een deelfunctor $J \subset \Lambda$ die voldoet aan de hieronder genoemde axiomas definieert een topologie op **C**.

H1. Als $R' \supset R \in J(X)$, dan $R' \in J(X)$,

H2. Als $R \in J(X)$, dan is $R^*_\Lambda J \in J(X)$.

(Hierbij is $R^*_\Lambda J$ het inverse beeld van J onder het, volgens het lemma van Yoneda, als functormorphisme $R: h_X \to \Lambda$ geïnterpreteerde element $R \in J(X) \subset \Lambda(X)$.)

F. Oort. Schoven en topologieën. Interuniversitair colloquim '64/'65.
M. Hazewinkel. Enkele opmerkingen over schoven en topologieën. Ibid.

9. Zij G een commutatieve eindige groep (multiplicatief geschreven) van exponent d; $\mathbf{Z}[G]$ de groep ring van G. Dan geldt:
$\sum_g a_g g$ is een eenheid in $\mathbf{Z}[G]$ desda $\varphi(\sum_g a_g g)$ een eenheid is in $\mathbf{Z}[\zeta_d]$ voor alle $\varphi \in \mathrm{Hom}_{\mathrm{Alg}}(\mathbf{Z}[G], \mathbf{Z}[\zeta d])$.
(ζ_d = een primitieve d^e-machts eenheidswortel).

10. De hypothese 'God', als basis voor een wereldverklaring, voldoet niet aan 'Occam's razor' ('entia non sunt multiplicanda praeter necessitatem').

J. Hospers. An introduction to philosophical analysis p. 287. Routledge & Kegan Paul, 1956.

11. Spellingsvereenvoudigingen verlagen de 'redundancy' van een gegeven tekst; een tekst met zeer lage 'redundancy' is echter moeilijk leesbaar. Het is dus wenselijk dat men eerst meet bij welk percentage 'redundancy' het efficiëntst gelezen wordt alvorens over te gaan tot het invoeren van een nieuwe spelling.

P. Guiraud. Language et la théorie de la communication. Encyclopédie de la Pleiàde. Language.

12. De ontwikkeling van een theorie kan eerder belemmerd dan bevorderd worden door het verzamelen van zeer grote aantallen feiten (bijv. metingen of losse stellingen)

M. Beckner. The biological way of thought. Univ. of Calif. Press, 1968. p.1.
A.N. Whitehead. Modes of thought. Capricorn Books, 1958.

13. 'De dwerg Monkel-Oor was een zeer belezen iemand die reeds jaren doende was de dikke Van Dale uit het hoofd te leren. Dit had zijn denkraam weliswaar niet verruimd, maar toch kwam zijn kennis soms handig van pas, zoals we zullen zien.'

M. Toonder. Heer Bommel en de wisselschat. 5567

'Kweetal: 'Ik wilde wel dat ik een groter denkraam had. Monkel-Oor heeft het helemaal volgepraat en nu het ik geen uitzicht meer."

ibid. 5568

Bovenstaande twee citaten geven een goed beeld van één van de moeilijkheden, waarmee student(e) en wetenschapsman dagelijks te maken hebben.

Stellingen behorende bij
het proefschrift van
M. Hazewinkel
Amsterdam, 1969

ABELIAN EXTENSIONS OF LOCAL FIELDS

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR IN DE WISKUNDE EN NATUURWETENSCHAPPEN AAN DE UNIVERSITEIT VAN AMSTERDAM, OP GEZAG VAN DE RECTOR MAGNIFICUS MR. A.D. BELINFANTE, HOOGLERAAR IN DE FACULTEIT DER RECHTSGELEERDHEID, IN HET OPENBAAR TE VERDEDIGEN IN DE AULA DER UNIVERSITEIT (TIJDELIJK IN DE LUTHERSE KERK, INGANG SINGEL 411, HOEK SPUI) OP WOENSDAG 18 JUNI 1969 DES NAMIDDAGS TE 16.00 UUR

DOOR

MICHIEL HAZEWINKEL

Geboren te Amsterdam

Druk: V.R.B.–Offsetdrukkerij – Kleine der A 3–4 – Groningen

1969

PROMOTOR: PROF. DR F. OORT
COREFERENT: MR DR A. MENALDA

0. INTRODUCTION. NOTATIONS AND CONVENTIONS.

(0.1) Introduction

Let K be a local field, i.e. a field with a discrete nonarchimedean absolute value, complete in the metric induced by this absolute value; suppose that the residue field k of K is perfect. The object of this study is a description of the abelian galois extensions L/K of K. (A galois extension is called abelian if its galois group is abelian.) Chapter I (= sections 1-4) contains the preparations for chapters II and III.

Suppose first that k is algebraically closed. One can give the group U(K) of units of K the structure of a pro-algebraic group over k (cf. (4.3)). Serre has shown in [CAC] that to every abelian finite extension of K there corresponds an isogeny of U(K) (i.e. an epimorphic map of pro-algebraic groups f: $U_f \to U(K)$ with finite kernel); and that esentially all isogenies of U(K) are obtained in this way. A generalisation of this theorem to the case that k is perfect but no longer necessarily algebraically closed is the subject matter of chapter II. The proof is an adaptation of Serre's proof in [CAC].

As to chapter III: suppose that k is a finite field. Exactly as in [LT] we start off by constructing some totally ramified extensions L_m/K of K; then we prove that they are abelian (without using formal groups; cf. (11.2)); next we more or less reverse the procedure of [LT] by proving first that the set of the L_m/K contains suficiently many totally ramified extensions (11.3), by means of a theorem on the norm map $U(L_m) \to U(K)$ (11.1.B), and then using this result to construct a reciprocity isomorphism (of which we prove that it is identical with the ('classical') reciprocity law isomorphism, given by the norm residue symbol, although we neither need nor use this fact).

The advantage of this approach (in the authors opinion) is that one can dispense with the rather involved machinery of local class field theory centring round the existence of a fundamental 2-cocycle. This method of obtaining the reciprocity isomorphism was suggested by Serre in [17] section 7; it is implicit in Dwork's description of the reciprocity isomorphism in [4] (cf. also [CL] Ch. XIII § 5), and of course in the results obtained by Lubin and Tate in [LT].

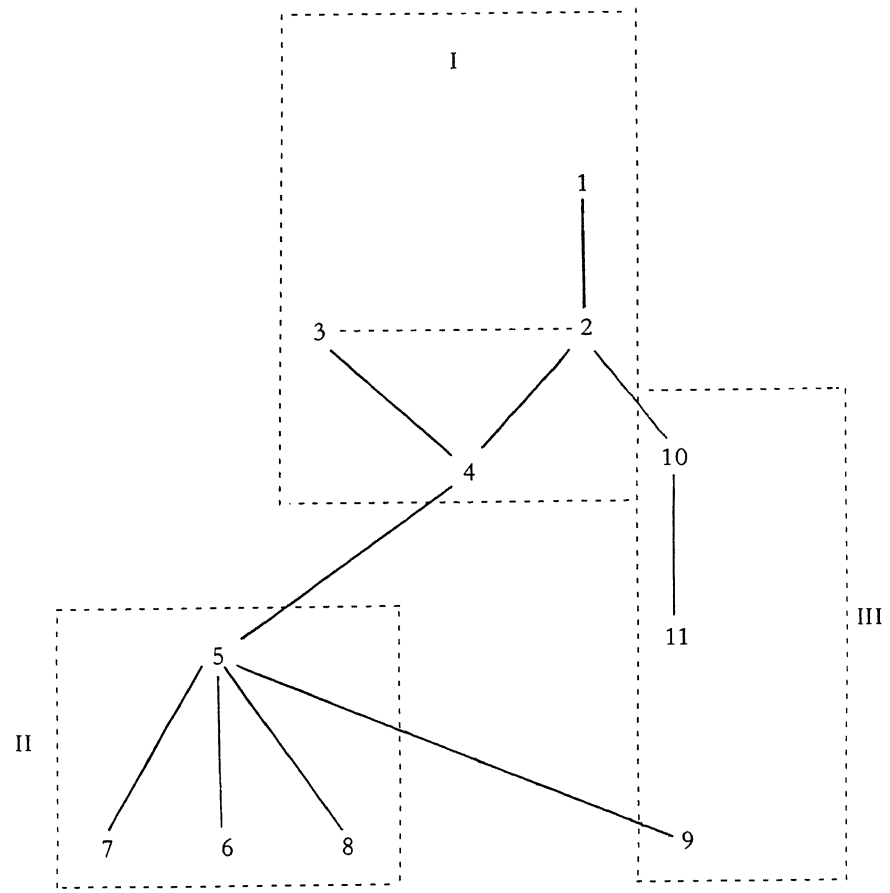
In fact the machinery needed for chapter III is rather modest. From the cohomology of groups and galois cohomology we only need that there exist such theories and a description of the cohomology groups in terms of cycles and boundaries. (Section 1 deals with this topic and some consequences bound up

with it.) As to local field theory: the first three chapters of Weiss's book [22] cover much more than we require in section 2 to prove some lemmas and propositions needed further down.
For chapter II we need in addition some general nonsense (treated in section 3) and some algebraic geometry connected with the definition of the homotopy groups of a pro-algebraic group (cf. [GP] and (4.5)) and with the Greenberg constructions ([CAC] §1, [6] §1, (4.2), (4.3)). (Section 4 deals with these matters.)
As indicated in (0.2) (interdependence of sections and chapters), chapter III is independant of chapter II and sections 3,4 of chapter I (except lemma (3.1)), although the considerations of sections 10, 11 were originally suggested by the results of chapter II. Cf. section 9 for further details on this point.

For a more detailed description of what happens in each chapter and section, the reader is referred to the brief introductory paragraphs heading each chapter and section.

Acknowledgements. From the introduction it has become clear that I am indebted to a large number of people. In particular, however, I have incurred a steadily increasing debt to Prof.Dr. F. Oort, who was the first to maintain that there ought to be a theorem like (5. 4. D), and without whose continuous interest and help this thesis would not have been written. Gratefull acknowledgement must be made to Prof. Dr. N.H. Kuiper who arranged my various duties in such a way that there was time enough to work on this thesis, as well as to Dr. A. Menalda who perused the manuscript carefully, which resulted in many suggestions for improvements.

(0.2) **Interdependence of sections and chapters**



(0.3) **Contents**

(0.4) Notations and conventions.

Convention. A commutative diagram will be called exact if all its rows and columns are exact.

Standard notations

$\mathbf{Z}$	: = integers.
$\mathbf{N}$	: = natural numbers.
$\mathbf{Q}$	: = rational numbers.
$\mathbf{R}$	: = real numbers.
$\mathbf{Q}_p$	: = field of p-adic numbers.
$\mathbf{Z}_p$	: = ring of p-adic integers.
$\mathbf{Z}/p\mathbf{Z}$	: = group of p elements.

Notations associated with a local field K.

$\lvert\ \rvert$	: = absolute value on K (and also its extension to an absolute value on an algebraic closure Ω of K).
v_K	: = normalized exponential valuation of K.
K^*	: = $K \setminus \{0\}$.
$A(K)$	: = ring of integers of K : = $\{x \in K \mid v_K(x) \geqslant 0\}$.
$\mathfrak{m}(K)$	: = maximal ideal of A(K) : = $\{x \in K \mid v_K(x) > 0\}$.
k	: = residue field of K (always assumed perfect; k : = $A(K)/\mathfrak{m}(K)$).
π_K	: = uniformizing element of K (i.e. $v_K(\pi_K) = 1$).
$U(K)$	: = $U^0(K)$: = group of units of $A(K) = \{x \in K \mid v_K(x) = 0\}$.
$U^n(K)$	: = $1 + \pi_K^n A(K)$. $n \geqslant 1$.
p	: = characteristic of k.
e	: = e_K : = $v_K(p)$ = : absolute index of ramification of K.
e_1	: = $e/(p-1)$.

Notations associated with extensions of a local field K.

Ω	: = fixed algebraic closure of K. All algebraic extensions of K are assumed to be contained in Ω.
K_{nr}	: = maximal unramified extension of K in Ω.
$\hat{K}_{nr}$	: = completion of K_{nr} (in a fixed completion $\hat{\Omega}$ of Ω).
K_{nr}^{ab}	: = maximal abelian unramified extension of K.

Let L/K be an extension of K.

$G(K,L \to \Omega)$	: = set of K-isomorphisms of L into Ω.
G(L/K)	: = set of K-automorphisms of L (= galois group of L/K when L/K is a galois extension).

$\mathfrak{a}_K$: = $G(K^{ab}/K_{nr}^{ab}) = G(K^{ab}/K)_{ram}$ = inertia subgroup of the galois-group of the maximal abelian extension of K.

$[L : K]$: = degree of L/K = dimension of L as a vectorspace over K.

K_L : = maximal unramified extension of K contained in L.

$G(L/K)_{ram}$: = $G(L/K_L) = : G(L/K)_0$ = inertia subgroup of G(L/K).

$G(L/K)_i$: = the i-th ramification subgroup of G(L/K).

$N_{L/K}$: = the norm map $L \to K$.

$Tr_{L/K}$: = the trace map $L \to K$.

$e_{L/K}$: = ramification index of L/K (= $[L : K_L]$).

$f_{L/K}$: = residue class degree of L/K (= $[K_L : K]$).

K_n : = unramified extension of degree n of K.

F : = Frobenius automorphism in $G(K_n/K)$ of an unramified extension K_n/K defined when the residue field of K is finite (or quasifinite).

Notations associated with abstract groups and the cohomology of groups.

#G : = number of elements of G

$<H, G>$: = subgroup of G generated by the elements of the form $h^{-1}g^{-1}hg$, $g \in G$, $h \in H$, where H is a subgroup of G.

$<G, G>$: = commutator subgroup of G.

G^{ab} : = $G/<G, G>$

Z(G) : = center of the group G.

$\mathbf{Z}[G]$: = group ring of G.

I_G : = augmentation ideal of $\mathbf{Z}[G]$ (= kernel of the map $\mathbf{Z}[G] \to \mathbf{Z}$, $g \mapsto 1$ = set of all elements of $\mathbf{Z}[G]$ of the type $\sum_{g \in G} n_g(g-1)$, $n_G \in \mathbf{Z}$).

Let G act on an abelian group A as a group of automorphisms (i.e. A is a G-module).

A^G : = $\{ a \in A \mid g(a) = a \text{ for all } g \in G \}$

N : = the norm map $A \to A$, $a \mapsto \sum_{g \in G} g(a)$.

$\hat{H}^i(G, A)$: = the i-th cohomology group of G with coefficients in A, $i \in \mathbf{Z}$.

Notations having to do with algebraic group schemes and pro-algebraic groups.

CG_k : = the category of commutative algebraic group schemes over k.

$Pro(CG_k)$: = the procategory of CG_k.

CQG_k : = category of commutative quasi-algebraic groups over k.

$Pro(CQG_k)$: = procategory of CQG_k.

$CCQG_k$: = the category of commutative, constant, quasi-algebraic groups over k.

$FCQG_k$	: = the category of finite, commutative, quasi-algebraic groups over k.
X^o	: = the connected component of the identity of X, $X \in CQG_k$, $Pro(CQG_k)$.
$\pi_0(X)$	: = X/X^o, $X \in CQG_k$, $Pro(CQG_k)$.
$\pi_1(X)$	: = first homotopy group of X; (π_1 : = first derived functor of π_0).
$Q(X)$	: = maximal constant quotient of a (pro-)finite commutative quasi-algebraic group X.
$\mathfrak{n}(X)$	: = $Q(\pi_1(X))$, $X \in CQG_k$, $Pro(CQG_k)$.
Lie X	: = tangent Lie-algebra at the identity of X, $X \in CG_k$.
X_{red}	: = maximal reduced subgroup scheme of X, $X \in CG_k$.
X_{inf}	: = X/X_{red}, $X \in CG_k$.
S_k	: = the constant algebraic group scheme over k of an abstract group S.

CHAPTER I

PRELIMINARY CONSIDERATIONS IN LOCAL FIELD THEORY, GALOIS COHOMOLOGY AND ALGEBRAIC GEOMETRY

1. SOME GALOIS COHOMOLOGY

This section deals with what is needed in the sequel of the cohomology of groups and galois cohomology. The definition of the cohomology groups is given in (1.1). In (1.2)–(1.5) one finds some elementary properties and calculations. Section (1.6) contains the construction and proof of part of the low term exact sequence of the homology spectral sequence associated with a change of groups $G \to G/H$ (where H is a normal subgroup of G). This is done explicitly by constructing some cochains (i.e. without using spectral sequences). "Hilbert 90" is treated in (1.7). In (1.8) we use (1.6) to establish the nullity of $\hat{H}^{-2}$ and $\hat{H}^{-1}$ in some cases. Instead of sections (1.6), (1.8) one could use Tate's theorem:

> Let G be a finite group and A a G-module. Then, if $\hat{H}^q(G, A)$ is zero for two consecutive values of q, it is zero for all $q \in \mathbf{Z}$.

(Cf. for a proof e.g. [CL] Ch. IX § 5 Th. 8). We have preferred to use the treatment as discussed in (1.6) and (1.8), even though it yields less, because of its more elementary nature.

(1.1) Cohomology of groups

(1.1.A) FINITE GROUPS

Let G be a finite group; a (left) G-module A is an abelian group A on which G acts (on the left) as a group of automorphisms. One can define cohomology groups $\hat{H}^q(G, A)$ which form a cohomology theory (cf. [CL] Ch. VII, VIII for instance; an explicit description is given immediately below). In particular this means that if

$$0 \to A' \to A \to A'' \to 0 \tag{1.1.A.1}$$

is an exact sequence of G-modules, then there exists a long exact sequence:

$$\ldots \hat{H}^{q-1}(G,A'') \to \hat{H}^q(G,A') \to \hat{H}^q(G,A) \to \hat{H}^q(G,A'') \to \hat{H}^{q+1}(G,A') \to \ldots \tag{1.1.A.2}$$

The functors $\hat{H}^q(G,-)$ are zero on all so-called induced modules (= relatively projective = relatively injective). A module A is called *induced* if there exists a subgroup X of A such that $A = \sum_{g \in G} gX$, the sum being direct. One obtains an explicit description of the groups $\hat{H}^q(G, A)$ by taking the homology of the complex

$$\ldots \to \underset{-3}{\mathbf{Z}[G]^2 \otimes A} \xrightarrow{d_{-2}} \underset{-2}{\mathbf{Z}[G] \otimes A} \xrightarrow{d_{-1}} \underset{-1}{A} \xrightarrow{d_0} \underset{0}{A} \xrightarrow{d_1} \underset{1}{\mathrm{Hom}(\mathbf{Z}[G], A)} \xrightarrow{d_2} \underset{2}{\mathrm{Hom}(\mathbf{Z}[G]^2, A)} \to \ldots$$

(Both Hom and $\otimes$ in this complex are taken over $\mathbf{Z}$). The map $d_0 = N$ is given by $a \mapsto \sum_g ga$ (the norm map); d_n is given by the formula:

$$d_n f(g_1, \ldots, g_n) = g_1 f(g_2, \ldots, g_n) + \sum_{j=1}^{n-1} (-1)^j f(g_1, \ldots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \ldots, g_n) + (-1)^n f(g_1, \ldots, g_{n-1})$$

for $n \geqslant 1$. Because G is finite, one can view the elements of $\mathbf{Z}[G]^n \otimes A$ also as functions $x: G^n \to A$. The formula for d_{-n} $(n \geqslant 1)$ then becomes:

$$(d_{-n}x)(g_1, \ldots, g_{n-1}) = \sum_g g^{-1} x(g, g_1, \ldots, g_{n-1}) + \sum_{j=1}^{n-1} (-1)^j \sum_g x(g_1, \ldots, g_{j-1}, g_j g, g^{-1}, g_{j+1}, \ldots, g_{n-1}) + (-1)^n \sum_g x(g_1, \ldots, g_{n-1}, g).$$

(1.1.B) PROFINITE GROUPS

Let G be a profinite group, i.e. an abstract group which can be written as a directed projective limit of finite groups (with the induced topology) and A a G-module. We suppose that the action of G on A is continuous (discrete topology on A). That is: for all $a \in A$, $\{s \in G \mid s(a) = a\}$ must be an open subgroup of G. One can then define

$$\hat{H}^q(G, A) := \varinjlim \hat{H}^q(G/H, A^H)$$

where $A^H := \{a \in A \mid h(a) = a \text{ for all } h \in H\}$; H runs through all open subgroups of G (which are of finite index in G); and the maps in the above inductive limit are induced by the natural inclusions $A^H \subset A^{H'}$, if $H' \subset H$, which com-

mute with the actions of H and H′.
These cohomology groups define a cohomology theory for modules over a profinite group G on which G acts continuously. In particular, given a short exact sequence like (1.1.A.1), there results a long exact sequence like (1.1.A.2).

(1.2) The chomology groups in dimensions $-1,0$

The map $d_0 : A \to A$ is the norm map N. To an element $g \otimes a$ of $\mathbf{Z}[G] \otimes A$ corresponds the function x on G given by $x(g) = a$ and $x(g') = 0$ if $g \neq g'$. One has $d_{-1}(x) := g^{-1}x(g) - x(g) = g^{-1}a - a$. Let I_G be the ideal of $\mathbf{Z}[G]$ consisting of all elements of the form $\sum_g n(g)\,(g-1)$, $n(g) \in \mathbf{Z}$. (The ideal I_G is the socalled augmentation ideal, i.e. the kernel of the homomorphism $\mathbf{Z}[G] \to \mathbf{Z}$ given by $\Sigma n(g)\,G \mapsto \Sigma n(g)$). Then, one has according to the definition in (1.1):

$$\hat{H}^{-1}(G, A) = \operatorname{Ker} N / I_G A \tag{1.2.1}$$

and

$$\hat{H}^{0}(G, A) = A^G / \operatorname{Im} N \tag{1.2.2}$$

where $A^G := \{a \in A \mid ga = a \text{ for all } g \in G\}$.

(1.3) The case: G is cyclic

Suppose that the group G is cyclic; let s be a generator of G. We define the following complex C(A) for all G-modules A:

$$C(A):\ \cdots \to A \xrightarrow{s-1} A \xrightarrow{N} A \xrightarrow{s-1} A \xrightarrow{N} A \to \cdots$$
$$\qquad\qquad -2 \qquad -1 \quad 0 \qquad 1 \quad 2$$

One can also construct a cohomology theory by taking the homology of these complexes. This cohomology theory coincides with the one defined in (1.1) in dimensions $0, -1$ (cf. also (1.2)), and is also zero on induced modules (of which there are sufficiently many). Therefore the two cohomology theories are isomorphic, and there results:

(1.3.A) *Proposition*

> If G is a finite cyclic group, then the sequence of cohomology groups $\hat{H}^q(G, A)$ is periodic of order two for every G-module A.

(1.4) **Interpretation of $\hat{H}^2(G, A)$ as a group of extensions.**

Let $\{1\} \to A \to E \to G \to \{1\}$ be an extension of groups (not necessarily commutative); let $s: G \to E$ be a system of representants of G in E. One can define an action of G on A by $g(a) := s(g) \,.\, a \,.\, s(g)^{-1}$. This definition does not depend on the choice of s, as A is commutative.
The elements $s(g) \,.\, s(g')$ and $s(gg')$ are in the same class of E mod. A, therefore there exists an $f(g, g')$ in A such that

$$s(g) \,.\, s(g') = f(g, g') \,.\, s(gg'). \tag{1.4.1}$$

Using the associativity of the multiplication in E one now proves by direct calculation that for every triple $g, g', g'' \in G$,

$$gf(g', g'') - f(gg', g'') + f(g, g'g'') - f(g, g') = 0, \tag{1.4.2}$$

i.e. that f is a cocycle.
Inversely given such a cocycle, one uses the formula (1.4.1) to define a multiplication in the set $E := A \times G$ (with s the natural section). The relation (1.4.2) then guarantees the associativity of this multiplication; and we obtain an extension $\{1\} \to A \to E \to G \to \{1\}$ of groups. It turns out that two extensions are isomorphic if and only if the corresponding cocycles are homologous. This means that we have found for every G-module A an isomorphism

$$\mathrm{Ext}(G, A) \xrightarrow{\sim} \hat{H}^2(G, A) \tag{1.4.3}$$

where the group on the left consists of only those extensions of G by A such that the induced action of G on A (as described above) is precisely the action of G on A as a G-module.
An extension $\{1\} \to A \to E \to G \to \{1\}$ is called *central* if $A \subset Z(E)$ (= centre of E). Such extensions correspond by the above to elements of the group $\hat{H}^2(G, A)$, where the action of G on A is trivial.

(1.5) **Calculation of $\hat{H}^{-2}(G, \mathbf{Z})$.**

Let G operate trivially on $\mathbf{Z}$. We have an exact sequence of G-modules

$$0 \to I_G \to \mathbf{Z}[G] \xrightarrow{\epsilon} \mathbf{Z} \to 0 \tag{1.5.1}$$

where I_G is the kernel of the map $\varepsilon: \mathbf{Z}[G] \to \mathbf{Z}$ given by $g \mapsto 1$ for all $g \in G$. (I.e. I_G is the collection of all elements of the form $\sum_g n(g)(g-1), n(g) \in \mathbf{Z}$). The

G-module $\mathbf{Z}[G]$ is free, hence induced. Using the long exact sequence associated with (1.5.1) there results an isomorphism

$$\hat{H}^{-2}(G, \mathbf{Z}) \xrightarrow{\sim} \hat{H}^{-1}(G, I_G).$$

Now $\hat{H}^{-1}(G, I_G) = \operatorname{Ker} N/I_G \cdot I_G = I_G/I_G^2$ (cf. (1.2)).
Furthermore the homomorphism defined by $s \mapsto \overline{s-1} \in I_G/I_G^2$ induces an isomorphism

$$G/\langle G, G\rangle \xrightarrow{\sim} I_G/I_G^2$$

as is easily checked. ($\langle G, G\rangle$:= commutator subgroup of G). Composing these isomorphisms yields:

(1.5.2) $$\hat{H}^{-2}(G, \mathbf{Z}) \xrightarrow{\sim} G/\langle G, G\rangle =: G^{ab}$$

We shall usually identify these two groups in the following.

(1.6) An exact sequence for $\hat{H}^{-2}$.

Let A be a G-module; H a normal subgroup of G. Consider the sequence

(1.6.1) $$\hat{H}^{-2}(H, A) \xrightarrow{a} \hat{H}^{-2}(G, A) \xrightarrow{b} \hat{H}^{-2}(G/H, A/I_H A) \to 0,$$

where a is the homomorphism induced by the homomorphism a', which assigns to a (-2)-chain $f: H \to A$ the chain $f': G \to A$ given by $f'|H = f$, $f'|G\backslash H := 0$; b is induced by the map *b* which assigns to a (-2)-chain $f: G \to A$ the chain *f*: $G/H \to A/I_H A$ given by $f(gH) := \sum_{h \in H} f(gh)$.

(1.6.A) *Proposition*

The sequence (1.6.1) is exact.

We proof this by means of several lemmas below.

Remark: (1.6.1) is in fact part of the low term exact sequence of the homology spectral sequence associated with the change of groups $G \to G/H$, cf. [2] Ch. XVI § 6 (4a).

(1.6.B) *Lemma*

A (-2)-chain $f: G \to A$ such that $(f|G\backslash\{e\}) = 0$ is a boundary.

Proof. Define $x: G^2 \to A$ by $x(e,e) := f(e)$, $x(g,g') := 0$ if $(g,g') \neq (e,e)$. Then $dx = f$ as is easily checked.

q.e.d.

(1.6.C) *Lemma*

Let $f: G \to A$ be a (-2)-chain; let $g_1 \notin H$ and suppose that $\sum_{h \in H} f(g_1 h) \in I_H A$. Then there exists a boundary dx such that $dx = f$ on $g_1 H$ and $dx = 0$ on $G \setminus H \setminus g_1 H$.

Proof. Let $\sum_{h \in H} f(g,h) = \Sigma h^{-1} a(h) - \Sigma a(h)$. We define $x: G^2 \to A$ by the formulas:

$x(h, g_1) := a(h)$ if $h \in H$.

$x(g_1, h) := -a(h')$ if $h \in H$, where $h' = g_1 h g_1^{-1}$.

$x(g_1 h, h^{-1}) := f(g_1 h)$ if $h \in H \setminus \{e\}$.

$x(g,g') := 0$ in all other cases.

Then we have

$$dx(g_1) = \sum_{g \in G} g^{-1} x(g, g_1) - \sum_{g \in G} x(g_1 g, g^{-1}) + \sum_{g \in G} x(g_1, g) =$$

$$= \sum_{h \in H} h^{-1} a(h) - \sum_{h \in H \setminus \{e\}} f(g_1 h) - \sum_{h \in H} a(h') = f(g_1),$$

and for $h \neq e$

$$dx(g_1 h) = \Sigma g^{-1} x(g, g_1 h) - \Sigma x(g_1 hg, g^{-1}) + \Sigma x(g_1 h, g)$$

$$= 0 - (a(g_1 h g_1^{-1}) - a(g_1 h g_1^{-1})) + f(g_1 h) = f(g_1 h).$$

For $g' \in G \setminus H \setminus g_1 H$ one sees in the same way by direct calculation that $dx(g') = 0$.

q.e.d.

(1.6.D) PROOF OF THE EXACTNESS OF THE SEQUENCE (1.6.1)

(i) surjectivity of b. Let $f: G/H \to A/I_H A$ be a cycle. We can assume $f(e) = 0$ (1.6.B). Choose a system of representants R of $G/H \setminus \{e\}$ in G. Define x': $G \to A$ by $x'(g) :=$ any lift of $f(\bar{g})$ if $g \in R$; $x'(g) := 0$ everywhere else. (as usual $\bar{g}$ denotes the image of $g \in G$ under the natural homomorphism $G \to G/H$). We have for x' that $\Sigma g^{-1} x'(g) - \Sigma x'(g) \in I_H A$ because f is a cycle. Let $\sum_g g^{-1} x'(g) -$

$\Sigma_g x'(g) = -\Sigma_{h\in H} h^{-1}a(h) + \Sigma_{h\in H} a(h)$; define $x: G \to A$ by $x := x'$ on $G \setminus H$ and $x(h) = a(h)$ if $h \in H$. Then x is a cycle and $b(x)$ is equal to f except possibly in e. A second application of (1.6.B) concludes this part of the proof.
(ii). The image of a cycle under the composed map $b\,a'$ is concentrated in e and hence represents zero (1.6.B). Therefore $b\,a = 0$.
(iii) Ker $b \subset$ Im a. Let $f: G \to A$ be cycle such that $b(f)$ is a boundary dy. By lifting y we can change f by a boundary in such a way that $b(f) = 0$ after this change; i.e. for all $g \in G$ we then have $\Sigma_{h\in H} f(gh) \in I_H A$. Applying (1.6.C) repeatedly we can now change f in a cycle concentrated on H; i.e. in a cycle of type $a'(z)$ for some cycle $z: H \to A$.

q.e.d.

(1.7) "Hilbert 90".

Let L/K be a finite galois extension with the galois group $G := G(L/K)$. The group G acts on the group L^* of non-zero elements of L.

(1.7.A) *Proposition.*

$$\hat{H}^1(G, L^*) = 0$$

Proof. Let $s \mapsto a_s$ be a 1-cocycle. For all $c \in L$ consider the element $b := \Sigma_s a_s s(c)$. There exists an element $c \in L$ such that $b \neq 0$ (linear independence of automorphisms of L/K; cf. [11] Ch. 1 Th. 3). Take such a c, then we have

$$t(b) = \sum_{s\in G} t(a_s)\, ts(c) = \Sigma\, a_t^{-1} a_{ts}\, ts(c) = a_t^{-1} b.$$

($t(a_s) = a_t^{-1} a_{ts}$ is the cocycle condition). One has $a_t = b/t(b)$, i.e. $t \mapsto a_t$ is a coboundary.

(1.7.B) *Remark.*

According to (1.3) this means also that $\hat{H}^{-1}(G, L^*) = 0$ in the case that G is cyclic, which is the classical form of "Hilbert 90". For a direct proof of this fact cf. e.g. [9] § 13 Satz 114.

(1.8) **Nullity of $\hat{H}^{-1}$ and $\hat{H}^{-2}$ if the norm map is surjective.**

Consider all finite galois extensions of a fixed field K. Suppose that the following condition is satisfied.

(1.8.1) For all finite galois extensions E, F such that $F \subset E$ is the norm map $N_{E/F}: E \to F$ surjective.

(1.8.A) *Proposition.*

Under condition (1.8.1) $\hat{H}^{-1}(G, L^*) = 0$ for all finite abelian extensions L/K.

Proof. In view of (1.7.B) we know that $\hat{H}^{-1}(G, L^*) = 0$ for cyclic extensions L/K. According to its definition $\hat{H}^{-1}(G, L^*) := \operatorname{Ker} N/I_G L^*$ (1.2). We proceed by induction on the number of elements of $G := G(L/K)$. The case $\#G = 1$ is trivial. Let H be a cyclic subgroup of G; L' the invariant field of H. Let N' and N'' be the norm maps

$$L \xrightarrow{N'} L' \xrightarrow{N''} K, \qquad N'' \circ N' = N.$$

Suppose $a \in L$ and $a \in \operatorname{Ker} N$, then $N''(N'(a)) = 1$. It follows from the induction hypothesis that there are $y_{\bar{s}}$ such that:

$$N'(a) = \prod_{\bar{s}} \frac{\bar{s}(y_{\bar{s}})}{y_{\bar{s}}}, \qquad \bar{s} \text{ running through } G(L'/K).$$

Let s be lift of $\bar{s}$; $y_s = y_{\bar{s}}$; choose x_s such that $N'(x_s) = y_s$. Then

$$N'(a) = \prod \frac{sy_s}{y_s} = \prod \frac{sN'(x_s)}{N'(x_s)} = N'\left(\prod \frac{sx_s}{x_s}\right) = N'(b);$$

i.e. $N'(a/b) = 1$. According to the proposition in the cyclic case there exist $z_t \in L$ for $t \in H$, such that

$$\frac{a}{b} = \prod \frac{tz_t}{z_t}, \qquad \text{i.e.} \qquad a = \prod_t \frac{tz_t}{z_t} \cdot \prod_s \frac{sx_s}{x_s} \in I_G L^*$$

q.e.d.

(1.8.B) *Lemma*

Let L/K be a finite abelian extension and suppose that (1.8.1) is satis-

fied. Let M be a subextension of L: $H \subset G$ the corresponding subgroup. Then $M^* \simeq L^*/I_H L^*$ as G/H-modules.

Proof. $N_{L/M}: L^* \to M^*$ is a surjective map of G-modules; the kernel is equal to $I_H L^*$ (1.8.A). Therefore $M^* \tilde{\leftarrow} L^*/I_H L^*$ as G-modules and also as G/H-modules for H acts trivially on M^*, whence on both.

q.e.d.

(1.8.C) *Proposition.*

$\hat{H}^{-2}(G, L^*) = 0$ for all abelian finite L/K if the hypothesis (1.8.1) is fulfilled.

Proof. For the cyclic case this follows from (1.3). The general case results from this by induction by means of the exact sequence (1.6.1).

q.e.d.

(1.8.D) *Remarks.*

1. Propositions (1.8.A) and (1.8.C) are stated only for abelian L/K. The same proofs, however, work for solvable L/K.
2. One can also conclude directly from $\hat{H}^1(G, L^*) = 0 = \hat{H}^0(G, L^*)$ that $\hat{H}^q(G, L^*)$ is zero for all q (by using the theorem, due to Tate, that all these cohomology groups are zero if two consecutive groups are zero; see e.g. [CL] Ch. IX § 6 Th. 8.)
3. The hypothesis (1.8.1) is satisfied in the case that K is a local field with algebraically closed residue field; cf. section (2.6).

2. SOME LOCAL FIELD THEORY.

Notation: From now on K denotes a local field with perfect residue field k; K_{nr} is the maximal unramified extension of K (in a fixed algebraic closure Ω of K), with residue field k_s, which is an algebraic closure of k; $\hat{K}_{nr}$ is a completion of K_{nr}; the symbol $|\ |$ denotes the absolute value on K, and also its extension to Ω. We use v or v_K to denote the normalized exponential valuation on K; finally π_K is a uniformizing element of K (i.e. $v_K(\pi_K) = 1$).
If L/K is a finite extension, K_L denotes the maximal unramified extension of K contained in L; $e_{L/K}$ is the ramification index of L/K (thus $e_{L/K} = [L : K_L]$).
In this section we define some assorted notions associated with local fields and

prove some propositions concerning them. In (2.1) we look at finite extensions of $\hat{K}_{nr}$ and show by means of Krasner's lemma that every such extension comes from an extension of some K_n, which is a finite unramified extension of K. In (2.2) we prove a fundamental lemma due to Lubin and Tate [LT], and apply this to deduce a result on the p-th roots of unity (p = char(k)), which could also have been obtained as a corollary to the study of the map $x \mapsto x^p$ carried out in (2.3). Section (2.4) gives a characterization of tamely ramified extensions which are also totally ramified. In (2.5) we define ramification groups, with the help of which the norm map is studied in (2.6). These two sections are simply a condensed and abbreviated version of the parts of chapters IV and V of [CL], which are needed further down. In (2.7) we establish a fundamental exact sequence, which occurs again and again in some form or another throughout this thesis. The section closes with (2.8) where in fact we prove that the ramified part of any abelian extension of K "comes from" some totally ramified abelian extension; in other words we prove that there are sufficiently many totally ramified abelian extensions (2.8.F).

(2.1) Extensions of $\hat{K}_{nr}$.

(2.1.A) *Krasner's lemma.*

Let $\alpha \in \Omega$; $r := \min |s(\alpha) - \alpha|$ where s runs through the set $G(K, K(\alpha) \to \Omega) \setminus \{1\}$ of all K-isomorphisms $K(\alpha) \to \Omega$ not equal to the identity. Suppose $\beta \in \Omega$ is such that $|\alpha - \beta| < r$. Then $G(K(\beta), K(\alpha, \beta) \to \Omega) = \{1\}$ and, if α is separable over K, we have $K(\alpha) \subset K(\beta)$.

See e.g. [22] lemma 3–2–5 for a proof of this lemma.

(2.1.B) EXTENSIONS OF $\hat{K}_{nr}$.

There is only one way to extend the valuation of K_{nr} to a finite extension E of K_{nr}. Hence if L/K is finite galois the injective restriction homomorphism

$$G(\hat{L}_{nr}/\hat{K}_{nr}) \to G(L_{nr}/K_{nr}) \xrightarrow{\sim} G(L/K_L) = G(L/K)_{ram}$$

is an isomorphism.
Inversely let $E/\hat{K}_{nr}$ be a finite extension. Then using the continuity of the roots of a polynomial as the coefficients vary, we see from Krasner's lemma (2.1.A) that there exists a finite extension L/K_n for some finite unramified extension K_n/K, such that $E = \hat{L}_{nr} = L\hat{K}_{nr}$ and we can take L/K separable if E is separable over $\hat{K}_{nr}$.

(2.1.C) *Corollary*

Let L, L' be two finite separable extensions of K, such that $L\hat{K}_{nr} \subset L'\hat{K}_{nr}$ (in a fixed completion $\hat{\Omega}$ of the algebraic closure Ω of K), then $LK_{nr} \subset L'K_{nr}$.

Proof. Let $x \in L$ be a generating element of L. According to Krasner's lemma one can find an $x' \in L'K_m$ (for some finite unramified extension K_m of K) such that $LK_m = K_m(x) \subset K_m(x') \subset K_m L'$.

q.e.d.

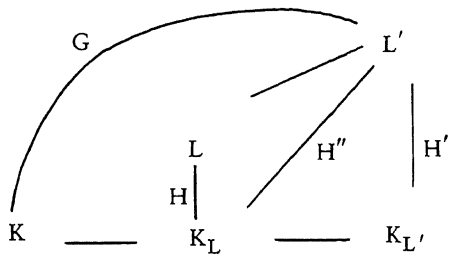
(2.1.D) *Lemma.*

For every finite abelian extension $E/\hat{K}_{nr}$ there exists a galois extension M/K such that:

(i) $G(M/K)_{ram}$ is abelian

(ii) $E \subset \hat{M}_{nr}$.

Proof. Let L be as in (2.1.B), and let L' be an arbitrary finite galois extension which contains L; let $G := G(L'/K)$; $H := G(L/K_L)$; $H' := G(L'/K_{L'})$; $H'' := G(L'/K_L)$; cf. the figure below.



$\langle H', H' \rangle$ is a normal subgroup of G (for $g^{-1}h_1^{-1}h_2^{-1}h_1h_2g = h_3^{-1}h_4^{-1}h_3h_4$, where $h_3 = g^{-1}h_1g$, $h_4 = g^{-1}h_2g \in H'$, for $g \in G$, $h_1, h_2 \in H'$).
Let M be the fixed field of $\langle H', H' \rangle$, then $G(M/K) \simeq G/\langle H', H' \rangle$ and $G(M/K)_{ram} \simeq H'/\langle H', H' \rangle$ is abelian; moreover for $s, t \in H''$, which contains H', we have $s^{-1}t^{-1}st(x) = x$ if $x \in L$ (the extension L/K_L is abelian). Therefore $L \subset M$.

q.e.d.

(2.2) **The basic Lubin-Tate lemma.**

Let K be a local field with finite residue field k; let q be the number of elements of k; let π_K be a uniformizing element of K. The symbol F_{π_K} denotes the set of all formal power series over A(K) (= $\{x \in K \mid v_K(x) \geqslant 0\}$ = ring of integers of K) such that

$$f \equiv \pi_K X \text{ mod. } X^2 \quad \text{and} \quad f \equiv X^q \text{ mod. } \pi_K .$$

(2.2.A) *Lemma ([LT] lemma 1).*

Let $f, g \in F_{\pi_K}$ be arbitrary. Then for every $a \in A(K)$ there exists exactly one power series $[a]_{f,g}$ with coefficients in A(K) such that

$$f \cdot [a]_{f,g} = [a]_{f,g} \cdot g \quad \text{and} \quad [a]_{f,g} \equiv aX \text{ mod. } X^2.$$

Proof. We define inductively polynomials F_r of degree r such that

$$f \cdot F_r \equiv F_r \cdot g \text{ mod. } X^{r+1} \quad \text{and} \quad F_r \equiv F_{r+1} \text{ mod. } X^{r+1}.$$

Take $F_1 = aX$; suppose that we have found F_r, $r \geqslant 1$; put $F_{r+1} := F_r + a_{r+1}X^{r+1}$ where a_{r+1} is yet to be determined.

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

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

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

$$a_{r+1} X^{r+1} \equiv \frac{f(F_r) - F_r(g)}{\pi_K^{r+1} - \pi_K},$$

which proves (inductively) that F_{r+1} is unique mod. X^{r+2} for all r, whence that $[a]_{f,g}$ is unique. It remains to show that $a_{r+1} \in A(K)$, which follows from

$$f(F_r) - F_r(g) \equiv F_r(X)^q - F_r(X^q) \equiv 0 \text{ mod. } \pi_K$$

$[a]_{f,g}$ is the limit of the F_r.

q.e.d.

(2.2.B) *Lemma.*

If a local field K (no restriction of the residue field) contains a primitive p-th root of unity ζ_p, then $v_K(\zeta_p - 1) = e/(p-1) := e_1$, (and e_1 is

therefore an integer). ($e := v_K(p)$ and $p := \mathrm{char}(k)$).

Proof. Let ζ_p be a primitive p-th root of unity; ζ_p is then a root of the irreducible polynomial $X^{p-1} + X^{p-2} + \ldots + X + 1$ and $\zeta_p - 1$ is a root of $(X+1)^{p-1} + (X+1)^{p-2} + \ldots + (X+1) + 1$, which is a polynomial of the type $X^{p-1} + p(\ldots) + p$. A root of such a polynomial has necessarily a v_K-value equal to $v_K(p)/(p-1)$.

q.e.d.

(2.2.C) *Application.*

Let K be a local field with algebraically closed residue field k of characteristic $p \neq 0$. Then the following are equivalent:

(i) e is divisible by $p-1$,

(ii) K contains a primitive p-th root of unity.

($e = \infty$ is by definition not divisible by $p-1$).

Proof. Lemma (2.2.B) proves (ii) $\Rightarrow$ (i). Suppose conversely that e is divisible by $p-1$; then there exists an element $u \in K$ with $v_K(u) = 0$ and such that $X^p - puX$ has a non-zero root. Let a be a $(p-1)$-th root of u (exists by Hensel's lemma because k is algebraically closed); then putting $Y := a^{-1}X$ we have a nonzero solution of $Y^p - pY = 0$. By (2.2.A) above there exists a power series h with coefficients in $\mathbf{Z}_p$ (= ring of p-adic integers) such that

$$h = Y + a_2 Y^2 + \ldots \quad \text{and} \quad h \cdot g = f \cdot h,$$

where $f := (Y+1)^p - 1$ and $g := Y^p - pY$. Then if b is a non-zero solution of $Y^p - pY = 0$, it follows that $1 + h(b)$ is a primitive p-th root of unity.

q.e.d.

(2.3) **The map $x \mapsto x^p$.**

We suppose $p := \mathrm{char}(k) \neq 0$ for the purpose of this section. Let $U^n(K) := 1 + \pi_K^n A(K)$; $U^0(K) := U(K) := A(K)^* = \{x \in K \mid v_K(x) = 0\}$. We consider the map $u: x \mapsto x^p$ of U(K) into itself.

(2.3.A) *Proposition*

u maps $U^n(K)$ into $U^m(K)$ and $U^{n+1}(K)$ into $U^{m+1}(K)$, where $m := np$ if $n \leqslant e_1$; $m := n + e$ if $n > e_1$. For the induced maps u_n:

$U^n(K)/U^{n+1}(K) \to U^m(K)/U^{m+1}(K)$ we have: $\ker u_n = 0$ if $n \neq e_1$ and $\ker u_{e_1} = \mathbf{Z}/p\mathbf{Z}$ or o depending on whether K contains all the p-th roots of unity or only the trivial one.

Proof. $n = 0$ is evident. Let $n \geqslant 1$ and $x = 1 + t\pi_K^n$, $t \in A(K)$ then $u(x) - 1 = pt\pi_K^n + \ldots + t^p\pi_K^{pn}$, where the v_K-value of any of the middle terms in the sum on the right is strictly larger than either $v(pt\,\pi_K^n) = v(t) + n + e$ or $v(t^p\pi_K^{pn}) = pv(t) + np$. This proves the first assertion of the proposition. If $1 \leqslant n < e_1$ then $u(x) \equiv 1 + t^p\pi_K^{np} \bmod U^{pn+1}(K)$. Under the isomorphisms $U^r(K)/U^{r+1}(K) \simeq k\,(r \geqslant 1)$ the map u_n then becomes $t \to t^p$, which has zero kernel (char(k) = p). If $n > e_1$ then $u(x) \equiv 1 + pt\,\pi_K^n \bmod. U^{n+e+1}(K)$. With the same identifications as above u_n now becomes $t \to at$ where a is some nonzero element of k. If $n = e_1$ we know that $\zeta \in U^{e_1}(K)$ if ζ is a p-th root of unity (2.2.B). Suppose on the other hand that $x \in U^{e_1}(K)$, $x^p \equiv 1 \bmod. U^{pe_1+1}(K)$; write $x = 1 + t\pi_k^{e_1}$. The monic equation

$$\pi_K^{-pe_1}\,[(\pi_K^{e_1}X + 1)^p - 1] = 0$$

then has a solution mod. π_K and it has simple roots mod. π_K (the derivative of the left hand side is equal to $\pi_K^{-pe_1}p\pi_K^{e_1} \not\equiv 0 \bmod. \pi_K$). Hence every element of the kernel of u_{e_1} can be refined to a p-th root of unity.

(2.4) Tamely ramified extensions.

A finite extension L/K is said to be *tamely ramified* if the residue extension l/k is separable and $p \nmid e_{L/K}$.

(2.4.A) *Proposition*

Suppose that L/K is both tamely and totally ramified. Let $[L : K] = e$. Then L is of the form $L = K(x)$ where x is a root of an equation $X^e = \pi_K$ for some uniformizing elements π_K of K.

See e.g. [22] Prop. 3–4–3 for a proof of this proposition.

(2.4.B) *Corollary.*

A tamely and totally ramified extension L/K of degree e is galois iff K contains all the e-th roots of unity.

(2.5) Ramification.

(2.5.A) DEFINITION OF THE RAMIFICATION GROUPS.

Let L/K be a finite galois extension with galois group G. We define the ramification subgroups G_i, $i = -1, 0, 1, 2, \ldots$ as follows:

$$G_i := \{s \in G \mid v_i(s(a) - a) \geqslant i + 1 \quad \text{for all} \quad a \in A(L)\}.$$

One proves easily that the G_i are normal subgroups of G, and that $G_i = \{1\}$ if i is large enough. ([CL] Ch. IV Prop. 1). One has

$$\text{(2.5.A.1)} \qquad \frac{su}{u} \in U^i(L) \quad \text{if} \quad s \in G_{i-1},\ u \in U(L);$$

$G_{-1} = G$; G_0 is the inertia subgroup of G and its invariant field is the maximal unramified extension K_L of K contained in L.

(2.5.B) THE TOTALLY RAMIFIED CASE.

We now suppose L/K to be totally ramified. Then a uniformizing element π_L of L generates A(L) as an A(K)-algebra; therefore we have in this case:

$$\text{(2.5.B.1)} \qquad \frac{s\pi_L}{\pi_L} \in U^i(L) \Leftrightarrow s \in G_i.$$

Define a map $G \to U(L)$ by the assignment $s \mapsto \frac{s\pi_L}{\pi_L}$. This map induces injections

$$\varphi_i : G_i/G_{i+1} \to U^i(L)/U^{i+1}(L),$$

which do not depend on the choice of π_L. (This follows from (2.5.A.1)). It follows that the φ_i are group homomorphisms.

$$\left(\varphi_i(st) := \frac{st\pi_L}{\pi_L} = \frac{st\pi_L}{t\pi_L} \cdot \frac{t\pi_L}{\pi_L} \equiv \frac{s\pi_L}{\pi_L} \cdot \frac{t\pi_L}{\pi_L} = \varphi_i(s) \cdot \varphi_i(t)\right).$$

The results (2.5.B.2) – (2.5.B.5) below derive from this fact with the help of the isomorphisms $U(L)/U^1(L) \simeq k^* = l^*$, $U^r(L)/U^{r+1}(L) \simeq k = l$ $(r \geqslant 1)$.

(2.5.B.2) If $\mathrm{char}(k) = 0$, then $G_1 = 0$, and every totally ramified extension of K is cyclic.

(k has no finite additive subgroups if char(k) = 0; finite subgroups of k^* are cyclic).

(2.5.B.3) If char(k) = $p > 0$, then G_0/G_1 is cyclic of order prime to p and G_1 is a p-group. (I.e. $\#G_1$ is a power of p.)

(2.5.B.4) The galois group of a totally ramified galois extension of a local field K (no restrictions on the residue field) is solvable.

Proof. There is a normal subgroup $G_1 \subset G_0 = G_{-1} = G$. The group G/G_1 is cyclic by the above, hence solvable; G_1 is a p-group and therefore solvable. The solvability of G itself follows.

q.e.d.

(2.5.B.5) The galois group of every finite galois extension of a local field with finite residue field is solvable.

Proof. The group G/G_0 is the galois group of an unramified extension, whence cyclic and therefore solvable. The group G_0 is solvable by (2.5.B.4).

q.e.d.

(2.5.C) *Proposition.*

Let L/K be a totally ramified abelian extension; char(k) = $p \neq 0$. Then G(L/K) is the direct product of a cyclic group of order prime to p and an abelian p-group.

Proof. There is an exact sequence $0 \to G_1 \to G \to G/G_1 \to 0$. The group G/G_1 is cyclic of order n prime to p. Let $\bar{s}$ be a generator of G/G_1; choose a lift s of $\bar{s}$; the element s^n is in G_1, so there exists a power q of p such that $(s^n)^q = 1$; the element $\bar{s}^q$ is also a generator of G/G_1; the homomorphism defined by $\bar{s}^q \to s^q$ is a section of the exact sequence above.

q.e.d.

(2.6) **The norm map.**

In this section L/K is a totally ramified cyclic extension of prime degree l, (unless otherwise stated).

(2.6.A) THE DIFFERENT (cf. [CL] Ch. III § 3)

Any uniformizing element π_L of L is a generator of A(L) over A(K). Let f be the minimal polynomial of π_L. Then the different of L/K is per definitionem equal to the ideal:

$$D = (f'(\pi_L)).$$

This different is characterized by the property:

(2.6.A.1) $$\delta \subset \mathfrak{a} D^{-1} \Leftrightarrow \mathrm{Tr}(\delta) \subset \mathfrak{a}.$$

($\mathfrak{a}$ an ideal of K, δ an ideal of L).
Let t be the number $t := v_L(s\pi_L - \pi_L) - 1$ (s a generator of $G = G(L/K)$). The number t is the largest integer such that $G_t = G$ (cf. (2.5)). Now $f'(\pi_L) = \prod_{s \neq 1} (\pi_L - s\pi_L)$, hence $v_L(f'(\pi_L)) = (l-1)(t+1)$, and we find that

(2.6.A.2) $$D = (\pi_L^m) \quad \text{with} \quad m = (l-1)(t+1).$$

(2.6.B) *Lemma.*

$$\mathrm{Tr}(\pi_L^n A(L)) = \pi_K^r A(K) \quad \text{with} \quad r = \left[\frac{(t+1)(l-1)+n}{l}\right] \quad (n \geqslant 0).$$

This follows immediately from the characterizing property of the different given above (2.6.A.1).

(2.6.C) *Lemma.*

$$\text{If } x \in \pi_L^n A(L), \text{ then } N(1+x) = 1 + \mathrm{Tr}(x) + N(x) \bmod \mathrm{Tr}(\pi_L^{2n} A(L)).$$

Proof. Define $x^a := \prod_{s \in a} s(x)$ for all finite subsets a of G. Then $N(1+x) = \sum_{a \subset G} x^a$.
Define $n(a) = \#a$. The terms of $N(1+x)$ with $n(a) = 0, 1, l$ are respectively 1, $\mathrm{Tr}(x)$, $N(x)$. If $n(a) \neq 0, 1, l$, then $sa \neq a$ for all $s \neq 1$ of G (for G is cyclic of prime order). Hence there exist $a_1, \ldots, a_r$ with $n(a_i) \geqslant 2$ for $i = 1, \ldots, r$ and such that

$$N(1+x) = 1 + \mathrm{Tr}(x) + N(x) + \sum_{i=1}^{r} \sum_{s} x^{sa_i}.$$

But $\sum_s x^{sa} = \mathrm{Tr}(x^a) \in \mathrm{Tr}(\pi_L^{2n} A(L))$ if $n(a) \geqslant 2$ and $x \in \pi_L^n A(L)$.

q.e.d.

Let ψ be the function defined by:

$$\psi(x) = x \qquad \text{if } x \leqslant t,$$

$$\psi(x) = t + l(x-t) \qquad \text{if } x \geqslant t.$$

(2.6.D) *Proposition.*

For all $n \geqslant 0$ one has:
(i) $N(U^{\psi(n)}(L)) \subset U^n(k)$ and $N(U^{\psi(n)+1}(L)) \subset U^{n+1}(K)$.
Let N_n be the induced map $U^{\psi(n)}(L)/U^{\psi(n)+1}(L) \to U^n(K)/U^{n+1}(K)$ and identify these quotients with k^* if $n = 0$ and with k if $n > 0$. Then we have for the maps N_n:
(ii) $N_0 : k^* \to k^*$ is given by $\xi \mapsto \xi^l$.
(iii) If $1 \leqslant n < t$; N_n is given by $N_n(\xi) = \alpha_n \xi^l$ for certain $\alpha_n \in k^*$.
(iv) If $1 \leqslant n = t$; $N_n : k \to k$ is given by $N_n(\xi) = \alpha\xi^p + \beta\xi$ for certain $\alpha \in k^*$, $\beta \in k$.
(v) If $n > t$; $N_n : k \to k$ is given by $N_n(\xi) = \beta_n \xi$ for certain $\beta_n \in k^*$.

Proof. Let $n = 0$. It is clear that (i) is true in this case. As L/K is totally ramified, it follows that N_0 is given by $\xi \mapsto \xi^l$.
$1 \leqslant n < t$. One has $\psi(n) = n$. Let $x \in \pi_L^n A(L)$, then $N(x) \in \pi_K^n A(K)$ because $v_K \circ N = v_L$. According to (2.6.B) one has $Tr(x) \in \pi_K^r A(K)$ with

$$r = \left[\frac{(t+1)(l-1)+n}{l}\right] \geqslant \left[\frac{(n+1)(l-1)+n+1}{l}\right] = n+1.$$

Analogously one proves that $Tr(\pi_L^{2n} A(L)) \subset \pi_K^{n+1} A(K)$. By virtue of (2.6.C) one then has $N(1+x) \equiv 1 + N(x) \bmod \pi_K^{n+1} A(K)$, which entails (i) in this case. Let $x = u\pi_L^n$, $u \in U(L)$, then $N(x) = u'N(\pi_L^n) = u''\pi_K^n$ for certain u'' in $U(K)$. This implies (iii) because $N(u) = u^l \bmod U^1(K)$ (which was also used in the case $n = 0$).
$1 \leqslant n = t$. Then $\psi(t) = t$. The same kind of calculations as in the previous case now yield $N(1+x) \equiv 1 + Tr(x) + N(x) \bmod \pi_K^{t+1} A(K)$ if $x \in \pi_L^t A(L)$. Whence (i) in this case and (iv).
$n > t$. Now $\psi(n) = t + l(n-t)$. In this case one finds that $N(1+x) \equiv 1 + Tr(x) \bmod \pi_K^{n+1} A(K)$, if $x \in \pi_L^n A(L)$, which proves (i) in this case and (v) except that possibly β_n could be zero. But if β_n were zero we would have $Tr(\pi_L^{\psi(n)} A(L)) \subset \pi_K^{n+1} A(K)$ which would contradict (2.6.B).

(This same argument can be used to prove that $\beta \neq 0$ in case (iv).)

q.e.d.

(2.6.E) *Corollary.*

If k is algebraically closed, $N(U^{\psi(n)}(L)) = U^n(K)$ and $N(U^{\psi(n)+1}(L)) = U^{n+1}(K)$ for all $n \geqslant 0$.

Proof. The second statement follows from the first because $\psi(n+1) \geqslant \psi(n) + 1$. The maps N_n are surjective for all $n \geqslant 0$ (2.6.D). Filtering U(L) by means of the $U^{\psi(n)}(L)$ and U(K) by means of the $U^n(K)$ we obtain the desired result as a consequence of the purely algebraic and elementary lemma (3.1) below.

q.e.d.

(2.6.F) *Corollary.*

$N(L^*) = K^*$, if k is algebraically closed.

(2.6.G) *Corollary.*

For all (totally ramified ((abelian) galois)) extensions L/K we have $N(U(L)) = U(K)$ and $N(L^*) = K^*$ if k is algebraically closed.

This follows from the transitivity of the norm maps and the solvability of the group G(L/K). (Cf. (2.5.B.4)).

(2.6.H) *Proposition.*

If L/K is any unramified galois extension, then

$$N_{L/K}U(L) = U(K) \Leftrightarrow N_{l/k}l = k.$$

(l/k is the residue field extension).

Proof. Because L/K is unramified one has $N_{L/K}(U^n(L)) \subset U^n(K)$ for all n. The induced maps $U^n(L)/U^{n+1}(L) \to U^n(K)/U^{n+1}(K)$ are the homomorphisms $N_{l/k} : l^* \to k^*$ for $n = 0$ and $Tr_{l/k} : l \to k$ for $n > 0$. The first of these statements follows from the fact that the reduction of the minimal polynomial of an element $x \in A(L)$ is the minimal polynomial of the reduction $\bar{x}$ of x; the

second is due to this same fact coupled with the formula

$$N(1 + \pi_K^n x) = \prod_s (1 + \pi_K^n s(x) = 1 + \pi_K^n \mathrm{Tr}(x) + \pi_K^{n+1}(\ldots) \quad (n \geqslant 1).$$

An application of lemma (3.1) concludes the proof.

q.e.d.

(2.6.J) *Corollary.*

Let K be a local field with finite (or quasi-finite) residue field. Then $N_{L/K}(U(L)) = U(K)$ for unramified extensions L/K, (and this is the case for unramified extensions only, cf. (10.2)).

(2.7) **The fundamental exact sequence.**

(2.7.A) Let K be a local field with algebraically closed residue field k. If E/F/K are finite galois extensions of K, we know that $N_{E/F}$ is surjective (2.6.G); i.e. the hypothesis (1.8.1) is fulfilled, which entails:

(2.7.A.1) $$\hat{H}^{-1}(G, L^*) = 0 = \hat{H}^{-2}(G, L^*). \qquad ((1.8.A), (1.8.C))$$

The exact sequence $o \to U(L) \to L^* \xrightarrow{v_L} \mathbf{Z} \to 0$ gives rise to a long exact sequence of cohomology groups

$$\cdots \to \hat{H}^{-2}(G, L^*) \to \hat{H}^{-2}(G, \mathbf{Z}) \to \hat{H}^{-1}(G, U(L)) \to \hat{H}^{-1}(G, L^*) \to \cdots$$

In (1.5) we showed that $\hat{H}^{-2}(G, \mathbf{Z}) \simeq G/\langle G, G\rangle$. Now write down the definition of $\hat{H}^{-1}(G, U(L))$ and use (2.7.A.1). The result is:

(2.7.A.2) If L/K is galois (k algebraically closed), the following sequence is is exact

$$0 \to G(L/K)^{ab} \xrightarrow{i} U(L)/V(L) \xrightarrow{N} U(K) \to 0$$

where, writing G for G(L/K), by definition, $V(L) := I_G U(L)$. The map i is given by:

(2.7.A.3) $$i : s \mapsto \frac{s\pi_L}{\pi_L}$$

which can be verified by tracing the various homomorphisms involved. This definition of i does not depend on the choice of π_L.

(2.7.B) THE GROUP V(L) IN A SPECIAL CASE.

Let L/K be totally ramified cyclic of prime order l. Let t be the largest integer such that $G_t = G$ (cf. (2.5)). Then the group V(L) is equal to

(2.7.B.1) $$V(L) = \mathrm{Ker}\, N_{L/K} \cap U^{t+1}(L).$$

Proof. It is clear that $V(L) \subset \mathrm{Ker}\, N$ and $V(L) \subset U^{t+1}(L)$ (2.5.A.1). By definition of t we have $\frac{s\pi_L}{\pi_L} \in U^t(L) \setminus U^{t+1}(L)$ for every $s \neq 1$ of $G(L/K)$, as $G = G(L/K)$ is cyclic of prime order. It follows from (2.7.A.2) that $\mathrm{Ker}\, N = i(G) \cdot V(L)$, where i is given by (2.7.A.3). Now $\frac{s\pi_L}{\pi_L} V(L) \subset U^t(L) \setminus U^{t+1}(L)$ for $s \neq 1$, owing to the fact that $\frac{s\pi_L}{\pi_L} \notin U^{t+1}(L)$ while $V(L) \subset U^{t+1}(L)$. Therefore $U^{t+1}(L) \cap \mathrm{Ker}\, N = V(L)$.

q.e.d.

(2.7.C) REMARK ON THE NON ALGEBRAICALLY CLOSED CASE.

If k is not algebraically closed $\hat{H}^{-1}(G, L^*)$ is not necessarily zero. For example take $K := Q_2$; let ζ_8 be a primitive 8-th root of unity; take $L := Q_2(\zeta_8)$; then $G(L/K) \simeq V_4$. One calculates that $\hat{H}^{-1}(G, L^*) \simeq \mathbf{Z}/(2)$. By the Tate theorem on group cohomology (cf. (1.8.D) Remark 2 or the introduction to section 2) this also shows that $N_{L/K}$ is not surjective in this case.

(2.8) **The pull-back theorem.**

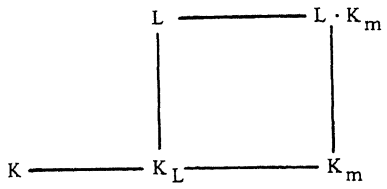
The symbol Z(G) denotes the centre of a group G.

(2.8.A) *Lemma.*

Let L/K be a finite galois extension; K_L the maximal unramified extension of K contained in L. Suppose that $G(L/K_L) \subset Z(G(L/K))$. Let K_m/K be any unramified galois extension containing K_L, then also $G(L \cdot K_m/K_m) \subset Z(G(L \cdot K_m/K))$.

Proof. Let $s \in G(L \cdot K_m/K_m)$ and $t \in G(L \cdot K_m)$. For $y \in K_m$ we have $ts(y) = t(y)$ and $st(y) = t(y)$ since also $t(y) \in K_m$. If $z \in L$ then $st(z) = ts(z)$ because of

$G(L/K_L) \subset Z(G(L/K))$. The field $L \cdot K_m$ is generated by L and K_m.



q.e.d.

(2.8.B) *Lemma.*

$\hat{H}^q(G(L/K), L) = 0$ for every galois extension L/K.

Proof. As a G-module L is induced on account of the normal basis theorem.

q.e.d.

(2.8.C) *Lemma.*

Let G be a finite abelian p-group and k a perfect field of characteristic p. Then

$$\hat{H}^q(G(k_s/k), G) = 0 \quad \text{for all} \quad q \in \mathbf{Z},$$

(trivial operation of $G(k_s/k)$ on G).

Proof. By induction on the number of elements of G. Let first $G \simeq \mathbf{Z}/p\mathbf{Z}$. There is an exact sequence of G-modules

$$0 \to \mathbf{Z}/p\mathbf{Z} \to k_s \to k_s \to 0$$

where the last map is given by $x \mapsto x^p - x$. Writing down the long exact sequence of this and applying (2.8.B) above gives the desired result in this case. For arbitrary G let H be a cyclic subgroup of order p; using induction and the long exact sequence belonging to $0 \to H \to G \to G/H \to 0$ one now proves the general case.

q.e.d.

(2.8.D) *Lemma.*

Let $\{1\} \to H \to G \xrightarrow{j} G/H \to \{1\}$ be an exact sequence of (not neces-

sarily commutative) groups. Suppose that there exists a section s of j, and that $H \subset Z(G)$. Then s(G/H) is a normal subgroup of G.

Proof. Let $g \in G$ be arbitrary; write $g = s(b)h$ where $h \in H$ and $b = j(g)$. Then $g^{-1}s(a)g = h^{-1}s(b)^{-1}s(a)s(b)h = h^{-1}s(b^{-1}ab)h = s(b^{-1}ab) \in s(G/H)$.

q.e.d.

(2.8.E) *Proposition.*

Let L/K be a finite galois extension. Then there exists a totally ramified extension L'/K such that $L \cdot K_{nr} = L' \cdot K_{nr}$.

Proof. Let K_L be the maximal unramified extension of K contained in L. Because $G(L/K_L)$ is solvable (2.5.B.4), it suffices to prove the proposition for the case that $G(L/K_L)$ is cyclic.
a) Let $q = \#G(L/K_L) \neq p = \mathrm{char}(k)$. Then $L = K_L(x)$ where x is a root of an equation $X^q = \pi$ for some uniformizing element $\pi \in K_L$ (2.4.A). As $X^q = u$ defines an unramified extension of K_L for any $u \in U(K_L)$, we can take $L' = K(x')$ where x' is a root of $X^q = \pi_K$, $\pi_K \in K$.
b) Let $\#G(L/K_L) = p$. Consider the canonical exact sequence

$$0 \to G(L/K)_{ram} \to G(L/K) \to G(K_L/K) \to 0$$

According to (2.8.C) we have $\varinjlim \hat{H}^2(G(K_n/K), G(L/K)_{ram}) = \hat{H}^2(G(K_{nr}/K), G(L/K)_{ram}) = \hat{H}^2(G(k_s/k), G(L/K)_{ram}) = 0$ where K_n/K runs through the unramified galois extensions of K. Hence for sufficiently large n there is a section s of

$$0 \to G(L/K)_{ram} \to G(L \cdot K_n/K) \to G(K_n/K) \to 0$$

Then $G(L \cdot K_n/K) = G(L/K)_{ram} \cdot s(G(K_n/K))$ (semidirect product). We can take $L' :=$ invariant field of $s(G(K_n/K))$.

q.e.d.

(2.8.F) *Corollary. (Pull-back theorem).*

Let L/K be a finite galois extension; K_L the maximal unramified extension of K contained in L, and suppose that $G(L/K_L) \subset Z(G(L/K))$, then there exists an abelian totally ramified extension L'/K such that

$$L' \cdot K_{nr} = L \cdot K_{nr}.$$

Proof. Let L' be as in (2.8.E), (2.8.A) and (2.8.D) now imply that L'/K is galois and hence abelian (because $G(L'/K)$ is isomorphic to $G(L/K_L)$.

(2.8.G) *Corollary.*

For every two totally ramified abelian extensions L/K, L'/K there exists a totally ramified extension M/K such that $M \cdot K_{nr} = L \cdot L' \cdot K_{nr}$.

(2.8.H) THE GROUP $\mathfrak{o}_K$.

Consider the projective system $\{G(L/K)_{ram} \mid L/K \in T\}$ indexed by the family T of all finite abelian extensions L/K of K (which are contained in some fixed algebraic closure Ω of K), with the ordening $L/K > L'/K$ iff $L \cdot K_{nr} \supset L' \cdot K_{nr}$, and the maps

$$G(L/K)_{ram} \xleftarrow{\sim} G(L_{nr}/K_{nr}) \to G(L'_{nr}/K_{nr}) \xrightarrow{\sim} G(L'/K)_{ram}$$

if $L/K > L'/K$. (Where the isomorphisms are the natural ones, and the middle map is the natural restriction.) This projective system is directed. Corollaries (2.8.G) and (2.8.F) show that

$$\mathfrak{o}_K := G(K^{ab}/K)_{ram} = \varprojlim G(L/K)_{ram} \tag{2.8.H.1}$$

where the projective limit is taken, either, over the above described projective system, or, over the directed subsystem (2.8.G) consisting of the totally ramified abelian L/K.

(2.8.J) *Corollary.*

For any local field with perfect residue field k we have

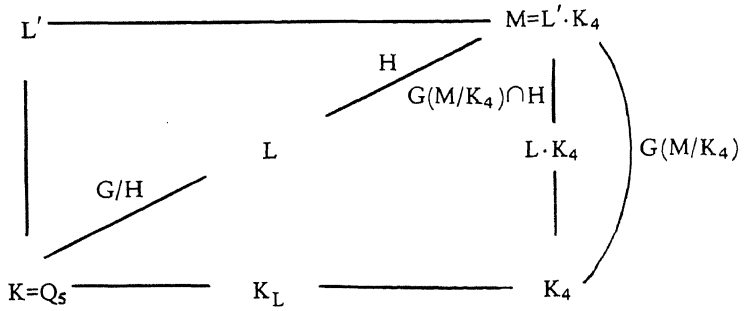
$$G(K^{ab}/K) \simeq G(K_{nr}^{ab}/K) \times \mathfrak{o}_K \simeq G(k^{ab}/k) \times \mathfrak{o}_K$$

This follows from (2.8.F). To determine the galois group $G(K^{ab}/K)$ we must therefore determine $G(k^{ab}/k)$, which may perhaps be considered an easier problem – especially when k is finite, quasi-finite of algebraically closed – and we must determine $\mathfrak{o}_K$. It is with another description of $\mathfrak{o}_K$ that chapter II is concerned.

(2.8.K) *Example.*

It is not true that every abelian extension L/K is the compositum of a totally ramified abelian extension L'/K and an unramified extension K_L/K.(According

to corollary (2.8.F) there is for every L/K an K_n/K such that this *is* true for the extension $L \cdot K_n/K)$. To construct a counterexample it suffices to find an abelian L/K such that $G(L/K_L)$ is not a direct summand.



Take $K = Q_5$; K_4 := unramified extension of degree 4 of Q_5 ; $L' := K(\zeta_5)$, where ζ_5 is a primitive 5-th root of unity; let $M := L' \cdot K_4$; then $G := G(M/K) \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Let $G(M/K_4)$ be the second factor; let H be the subgroup of order 4 generated by the element (2,1) of G(M/K). Let L be the invariant field of H. One now shows easily that $G(L/K) \simeq \mathbf{Z}/4\mathbf{Z}$ and that $G(L/K_L) \simeq \mathbf{Z}/2\mathbf{Z}$, which is not a direct summand.

(2.8.L) *Remarks.*

1. The requirement $G(L/K_L) \subset Z(G(L/K))$ means that G(L/K) is abelian in the case that the residue field of K is finite or quasi-finite (or algebraically closed).
2. In the case that the residue field k is finite (or quasi-finite) there is a much easier proof of (2.8.F) and (2.8.E) as follows. Let F be a generator of $G(K_L/K)$, take any lift s of F in G(L/K). The order n of s is a multiple of the order of F. Let K_n/K be the unramified extension of degree n of K. Then $K_n \supset K_L$. We also use F to denote a generator of $G(K_n/K)$ which restricts to the previous F on K_L. There is exactly one element t of $G(K_n \cdot L/K)$ which restricts to s on L and to F on K_n. The order of t is n. The homomorphism defined by $F \mapsto t$ gives a section of the exact sequence

$$0 \to G(L \cdot K_n/K)_{ram} \to G(L \cdot K_n/K) \to G(K_n/K) \to 0$$

$$(G(L \cdot K_n/K)_{ram} = G(L \cdot K_n/K_n)).$$

q.e.d.

3. SOME CATEGORY THEORY.

In this section, included mostly for completeness sake, we have collected some well-known algebraic and categorical facts used elsewhere. Section (3.1) contains a lemma on filtered abelian groups, which has already been used twice in section (2.6). In (3.2) we discuss procategories, and prove once more that the procategory of an abelian category is abelian (3.2.E). In (3.3) lastly we apply the results found to projective systems of finite abelian groups.

(3.1) **Lemma on filtered abelian groups** ([CL] Ch. V § 1 lemma 2).

> Let A (resp. B) be an abelian group filtered by subgroups $A = A_0 \supset A_1 \supset \ldots$ (resp. $B = B_0 \supset B_1 \supset \ldots$) such that $A = \varprojlim A/A_n$ and $\cap B_n = \{0\}$ (e.g. $B = \varprojlim B/B_n$). Let $u: A \to B$ be a morphism of filtered groups (i.e. a homomorphism such that $u(A_n) \subset B_n$) and let u_n: $A_n/A_{n+1} \to B_n/B_{n+1}$ be the induced homomorphism. Then:
> (i) u_n surjective for all $n \Rightarrow u$ is surjective
> (ii) u_n injective for all $n \Rightarrow u$ is injective.

Proof. From the fact that u_n is injective we deduce that $\mathrm{Ker}\, u \cap A_n = \mathrm{Ker}\, u \cap A_{n+1}$, hence inductively $\mathrm{Ker}\, u \subset A_n$ for all n, which proves (ii). Let $b \in B$ be arbitrary; u_0 is surjective, hence there is an $a_0 \in A$ such that $(u(a_0) - b) = b_1 \in B_1$; u_1 is surjective, hence there is an $a_1 \in A_1$ such that $(u(a_1) + b_1) = b_2 \in B_2$, i.e. $(u(a_0 + a_1) - b) \in B_2$; in this way one constructs a series $a_0 + a_1 + \ldots$; this series converges to an element $a \in A$; we have $(u(a) - b) \in B_n$ for all n, hence $u(a) = b$.

q.e.d.

(3.2) **Procategories.**

(3.2.A) DEFINITIONS.

Let C be an arbitrary category. We consider the procategory Pro(C) of C, of which the objects are all directed projective systems of C, and which has as morphisms from $(X_a)_{a \in A}$ to $(Y_b)_{b \in B}$ the set

$$\mathrm{Hom}_{\mathrm{Pro}(C)}((X_a),(Y_b)) := \varprojlim_b \varinjlim_a \mathrm{Hom}(X_a, Y_b).$$

Such a morphism is determined by giving for every $b \in B$ an $a(b) \in A$ and a

morphism $f_{a(b)}: X_{a(b)} \to Y_b$ (which represents f_b) such that if $b' > b$, there exists an $a > a(b), a(b')$ such that

$$(X_a \to X_{a(b')} \to Y_{b'} \to Y_b) = (X_a \to X_{a(b)} \to Y_b)$$

A directed partially ordered set A will be called *almost finite* if for every $a \in A$ there are only finitely many elements smaller than a. An object of Pro(C) will be called *almost finite* if its index set enjoys this property.

(3.2.B) THE AXIOMS OF ABELIANNESS IN A SPECIAL CASE.

We consider morphisms of a special type (E) in Pro(C). A morphism f is of type (E) if:

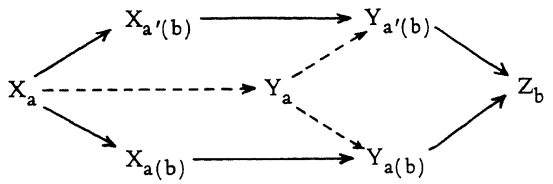
f is a morphism between objects of Pro(C) indexed by the same index set A: $f: (X_a) \to (Y_a)$ where f is given by morphisms $f_a: X_a \to Y_a$ such that

(E)
$$(X_{a'} \to Y_{a'} \to Y_a) = (X_{a'} \to X_a \to Y_a)$$

whenever $a' > a$.

Lemma. Let f be a morphism of type (E). Then:
(i) If all the f_a are monomorphic, so is f.
(ii) If all the f_a are epimorphic so is f.
Suppose in addition that C has a zero object and that the kernels K_a and cokernels C_a of f_a exist for all $a \in A$.
(iii) (K_a) is a kernel of f.
(iv) (C_a) is a cokernel of f.

Proof. (ii). Let $g = (g_b)$, $g' = (g'_b): (Y_a) \to (Z_b)$ be two morphisms such that $g \circ f = g' \circ f$. Let $g'_{a'(b)}: Y_{a'(b)} \to Z_b$ represent g'_b and $g_{a(b)}: Y_{a(b)} \to Z_b$ represent g_b. By hypothesis there exists an $a > a(b'), a > a(b)$ such that the following diagram commutes.



The dotted arrows exist by the hypothesis of the lemma. The morphism $X_a \to Y_a$

is epimorphic, hence $(Y_a \to Y_{a'(b)} \to Z_b) = (Y_a \to Y_{a(b)} \to Z_b)$; i.e. $g_b = g'_b$. (i) is proved analogously.
(iv). By (ii) $(Y_a) \to (C_a)$ is an epimorphism. Let $g: (Y_a) \to (Z_b)$ be a morphis such that $g \circ f = 0$. Let $g_{a(b)}: Y_{a(b)} \to Z_b$ represent g_b. By hypothesis there exists an $a \in A$ such that $(X_a \to Y_a \to Y_{a(b)} \to Z_b) = (X_a \to X_{a(b)} \to Y_{a(b)} \to$ 0, hence $Y_a \to Z_b$ factorizes through C_a. The morphisms $C_a \to Z_b$ so obtaine define the desired factorization of g. (iii) is proved analogously.

q.e.

(3.2.C) *Lemma.*

Every object of Pro(C) is isomorphic with an almost finite object.

Proof. Let $(X_a)_{a \in A}$ be any object of Pro(C). Consider the set S of all finite directed subsets of A. Each $s \in S$ has a largest element a(s). We partially orde S by $(s < s') \Leftrightarrow (s \subset s')$. It is clear that S is an almost finite partially ordered directed set. Define $X_s := X_{a(s)}$ for all $s \in S$; and $(X_{s'} \to X_s) := (X_{a(s')} \to X_{a($ if $s' > s$ (which implies $a(s') > a(s)$). Now define morphisms $f: (X_s) \to (X_a)$, $g: (X_a) \to (X_s)$ as follows: for each $s \in S$ let a(s) be the above defined elemen of A and define $g_{a(s)}: X_{a(s)} \to X_s$ as the identity; for each $a \in A$, let $s(a) := \{$ and define $f_{s(a)}: X_{s(a)} \to X_a$ as the identity. The maps f and g are inverses o each other.

(3.2.D) MORPHISMS INTO AN ALMOST FINITE OBJECT.

Let $f: (X_a) \to (Y_b)$ be a morphism into the almost finite object $(Y_b)_{b \in B}$. Le $B_n := \{b \in B \mid$ there are exactly n elements of B strictly smaller than $b\}$. We are going to determine inductively for every $b \in B$ an $a(b) \in A$ and a morphi $f_{a(b)}$ which represents f_b such that:

(3.2.D.1) Whenever $b' > b$, then $a(b') > a(b)$ and

$$(X_{a(b')} \to Y_{b'} \to Y_b) = (X_{a(b')} \to X_{a(b)} \to Y_b).$$

If $b \in B_0$, choose a(b) arbitrary such that there exists a representant $f_{a(b)}$ of f_b. Let $b \in B_n$, $n \geqslant 1$; let $b_1, \ldots, b_n$ be the n elements of B smaller than b. L $a'(b)$ be such there exists a representant $f_{a'(b)}$ of f_b. For every $i = 1, \ldots, n$ there exists an a_i larger than $a'(b)$ and $a(b_i)$, such that

$$(X_{a_i} \to X_{a'(b)} \to Y_b) = (X_{a_i} \to X_{a(b_i)} \to Y_{b_i}),$$

and there exists an a(b) larger than all the a_i such that all the $f_{a(b)} := (X_{a(b)} \to X_{a_i} \to X_{a'(b)} \to Y_b)$ (which all represent f_b) are equal. These a(b) and $f_{a(b)}$ satisfy the requirements of (3.2.D.1) by their definition.

Let $A' = \{a \in A \mid \exists\, b \in B \text{ such that } a > a(b)\}$. A' is cofinal in A, which implies that $(X_a)_{a \in A'}$ is naturally isomorphic to $(X_a)_{a \in A}$. Let T be the set $T := \{(a,b) \in A \times B \mid a > a(b)\}$ order T by $((a',b') > (a,b)) \Leftrightarrow (a' > a \text{ and } b' > b)$. Define the pro-objects $(X_t)_{t \in T}$, $(Y_t)_{t \in T}$ as follows: $X_t := X_a$ and $Y_t := Y_b$ if $t = (a,b)$; the morphisms are the natural ones. If we now define $f_t: X_t \to Y_t$ as $f_t := (X_a \to X_{a(b)} \to Y_b)$ $(t = (a,b))$, we have found, in view of the constructions above, a morphism of type (E) "isomorphic" to the original f. More precisely, taking account of (3.2.C), we have proved:

(3.2.D.2) *Lemma.*

For every morphism $f: (X_a) \to (Y_b)$ of Pro(C) there are objects (X_t), (Y_t) and a morphism of type (E) $(X_t) \to (Y_t)$, together with isomorphisms $(X_a) \xrightarrow{\sim} (X_t)$, $(Y_b) \xrightarrow{\sim} (Y_t)$ such that the following diagram commutes.

$$\begin{array}{ccc} (X_a) & \xrightarrow{\quad f \quad} & (Y_b) \\ \wr\downarrow & & \wr\downarrow \\ (X_t) & \longrightarrow & (Y_t) \end{array}$$

This means that we can replace isomorphically every morphism of Pro(C) by one of the special type discussed in (3.2.B).

(3.2.E) *Proposition.*

(i) If C is additive, so is Pro(C).
(ii) If C has enough kernels, so has Pro(C).
(iii) If C has enough cokernels, so has Pro(C).
(iv) If C is abelian, so is Pro(C).

Proof. (i) is clear; (ii) and (iii) follow from (3.2.B) and (3.2.D.2). To prove (iv) we have to show that finite products and sums exist in Pro(C), which is easy, and that the image and coimage of a morphism of type (E) are isomorphic. Let $I_a := \text{Ker}\,(Y_a \to C_a)$, $J_a := \text{Coker}\,(K_a \to X_a)$. The category C is abelian, the natural induced morphism $J_a \to I_a$ is therefore an isomorphism. It is clear that

these isomorphisms define an isomorphism of the pro-objects (J_a) and (I_a).

q.e.d.

(3.2.F) PROLONGATION OF FUNCTORS ON C.

Let C be an abelian category; and F: C → Ab (the category of abelian groups) a functor which has only finite groups as values. We can extend F to a functor Pro(F): Pro(C) → Ab by means of the definition

$$\mathrm{Pro}(F)\,((X_a)_{a\in A}) := \varprojlim F(X_a).$$

Lemma. If F is right exact on C, Pro(F) is right exact on Pro(C).

Proof. Let $(X_a) \to (Y_b) \to (Z_c) \to 0$ be a right exact sequence of Pro(C). By applying the procedure of (3.2.D) to the morphism $(X_a) \to (Y_b)$ and then taking the cokernel as in (3.2.B) we can change this sequence into an isomorphic sequence $(X_t) \to (Y_t) \to (Z_t) \to 0$ such that the diagram

$$\begin{array}{ccccccc} X_{t'} & \longrightarrow & Y_{t'} & \longrightarrow & Z_{t'} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ X_t & \longrightarrow & Y_t & \longrightarrow & Z_t & \longrightarrow & 0 \end{array}$$

is exact whenever $t' > t$. Now apply F to this diagram and use (3.3.A) below. The required result follows.

q.e.d.

(3.2.G) PROJECTIVE LIMITS IN PRO(C).

An object $\mathbf{X} = (X_a)_{a\in A}$ of Pro(C) is called *strict* if the morphisms $X_a \to X_{a'}$ are epimorphic for all $a > a'$.

Proposition. (i) Projective limits of projective systems consisting of strict pro-objects exist in Pro(C).
(ii) Arbitrary products exist in Pro(C) if finite products exist in C.

Proof. (ii) follows from (i), once one has proved that finite products exist in Pro(C), which is easy. As to (i), let $(\mathbf{X}_i, f_j^i, I)$ be a projective system consisting of strict pro-objects; write $\mathbf{X}_i = (X_{i_t})_{i_t\in T_i}$. Let S be the disjoint union of the

sets T_i, $i \in I$. We define an ordening $>$ on S as follows:

$i_t > j_{t'}$ $\quad$ $i > j$ and there exists a map $X_{i_t} \to X_{j_{t'}}$ which represents $(f^i_j)_{t'}$.

(when $i = j$ this means $t > t'$ in T_i).
The maps $X_{i_t} \to X_{j_{t'}}$ mentioned above define a projective system $(X_{i_t})_{i_t \in S}$. (One needs the strictness hypothesis to show that $(X_{i_t} \to X_{j_{t'}} \to X_{k_{t''}}) = (X_{i_t} \to X_{k_{t''}})$ if $i_t > j_{t'} > k_{t''}$). This projective system is the projective limit of (X_i).

q.e.d.

Remark. If we had taken a weaker ordening $>'$ on S, such that
1°. $(s >' s') \Rightarrow (s > s')$
2°. $(s > s') \Rightarrow (s'' > s$ such that $s'' >' s'$ and $s'' > s')$
then we would have obtained an isomorphic object $(X_s)_{s \in S}$.

(3.2.H) THE PROCATEGORY OF AN ARTINIAN ABELIAN CATEGORY.

In this section we suppose that C is abelian and that every object of C is artinian.

(3.2.H.1) Every object of Pro(C) is isomorphic to a strict object. (Under the conditions stated above).

Proof. Let $(X_t, f^{t'}_t, T)$ be an object of Pro(C). Let $Y_t := \bigcap_{t' > t} f^{t'}_t(X_{t'})$; on account of the fact that X_t is artinian, there is an $s(t)$ such that $X_{s(t)} \to X_t$ factorizes through Y_t, then so does $X_{t'} \to X_t$ for $t' > s(t)$, the induced map $X_{s(t)} \to Y_t$ is epimorphic, and so is $X_{t'} \to Y_t$ for every $t' > s(t)$; it follows that the system (Y_t) is strict. The inclusions $Y_t \to X_t$ and the epimorphisms $X_{s(t)} \to Y_t$ show that the systems (Y_t) and (X_t) are isomorphic.

q.e.d.

(3.2.H.2) Projective limits are exact in Pro(C). (Still under the conditions stated at the beginning of this subsection (3.2.H)).

Proof. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{i'} & \longrightarrow & B_{i'} & \longrightarrow & C_{i'} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0 \end{array}$$

be an exact diagram for every $i' > i$ of a partially ordered directed index set I. We can assume that all the objects A_i, B_i, C_i are strict. We can furthermore assume that each $0 \to A_i \to B_i \to C_i \to 0$ is given by exact sequences $0 \to A_{i_t} \to B_{i_t} \to C_{i_t} \to 0$ (apply the procedure of (3.2.D) to $B_i \to C_i$ and take the kernel as in (3.2.B and then take the cokernel of $(\mathrm{Ker}(B_i \to C_i) \to B_i)$ again as in (3.2.B). Because of strictness we have an exact diagram

(*)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{i_t} & \longrightarrow & B_{i_t} & \longrightarrow & C_{i_t} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{j_{t'}} & \longrightarrow & B_{j_{t'}} & \longrightarrow & C_{j_{t'}} & \longrightarrow & 0 \end{array}$$

whenever all these maps exist. As to their existence:

(**) for every $j_{t'}$ and $i > j$ there is an $i_t \in T_i$ such that all these maps exist.

As in (3.2.G) let S be the disjoint union of the T_i. We now define a some – what weaker ordering on S (than in (3.2.G)) as follows:

$$i_t > j_{t'} \Leftrightarrow i > j \text{ and all the maps of the diagram (*) above exist.}$$

The sequence of pro-objects $0 \to (A_s) \to (B_s) \to (C_s) \to 0$ obtained by taking this ordening on S is exact ((*) and (3.2.B)), while property (**) and the remark below (3.2.G) together insure that $(A_s) \simeq \varprojlim_i A_i$, $(B_s) \simeq \varprojlim_i B_i$ and $(C_s) \simeq \varprojlim_i C_i$.

q.e.d.

(3.3) Projective limits of finite abelian groups.

(3.3.A) *Lemma.*

Let T be a directed partially ordered set and (A_t), (B_t), (C_t) projective systems of finite abelian groups indexed by T. Suppose that the diagram

$$\begin{array}{ccccc} A_{t'} & \xrightarrow{f_{t'}} & B_{t'} & \xrightarrow{g_{t'}} & C_{t'} \\ {\scriptstyle r_t^{t'}}\downarrow & & \downarrow & & \downarrow \\ A_t & \xrightarrow{f_t} & B_t & \xrightarrow{g_t} & C_t \end{array}$$

is exact for every $t' > t$. Then the induced sequence of abelian groups

$$\varprojlim A_t \to \varprojlim B_t \to \varprojlim C_t$$

is exact.

Proof. That $g \cdot f = 0$ is trivial. Let $g((b_t)) = 0$. Let $X_t = f_t^{-1}(b_t)$ for all t. If we can show that there exists a point $(a_t) \in \varprojlim A_t$ such that $a_t \in X_t$ for all t we are through. Let S be the set of all families $(Y_t)_{t \in T}$, Y_t a subset of X_t and such that $r_t^{t'}(Y_{t'}) \subset Y_t$ for all $t' > t$. Order S by inclusion. The set S is not empty and every decreasing sequence of elements of S has a minimal element (finiteness of the X_t!). Let (Z_t) be a minimal element of S (Zorn's lemma)). Owing to the minimality of (Z_t) it follows first that $r_t^{t'}(Z_{t'}) = Z_t$ for all $t' > t$, and then that each Z_t consists of only one element z_t. The element (z_t) is the required element of $\varprojlim A_t$.

q.e.d.

Remark. Suppose that the abelian groups A_t, B_t, C_t are no longer necessarily finite, but that we have given instead for every t a set S_t of subsets of A_t such that $f_t^{-1}(b) \in S_t$ for every $b \in B_t$ and $r_t^{t'}(E) \in S_t$ for every $E \in S_{t'}$, $t' \geqslant t$, and such that the sets S_t, partially ordered by inclusion, enjoy the descending chain property. Also in this case it follows that the sequence of abelian groups

$$\varprojlim A_t \to \varprojlim B_t \to \varprojlim C_t$$

is exact. The proof is exactly the same except that all the Y_t must be in S_t. The situation described above occurs for instance in the case that the A_t (resp. B_t, C_t) are the groups of k_s-points of quasi-algebraic groups F_t (resp. G_t, H_t) over a base field k and the f_t, g_t derive from morphisms of quasi-algebraic groups. For the set S_t we can then take the set of all subsets of the form $x + F'(k_s)$ of $A_t = F_t(k_s)$, where $x \in A_t$ and F_t' is a quasi-algebraic subgroup of F_t. The partially ordered set S_t satisfies the descending chain condition because F_t is artinian (i.e. satisfies the descending chain condition for quasi-algebraic subgroups.)

(3.3.B) *Lemma.*

Let $f(X_a) \to (Y_b)$ be a map of projective systems of finite abelian groups. Suppose that:

1°. For every $b \in B$ there is an $f_{a(b)}: X_{a(b)} \to Y_b$ representing f_b which is surjective.

2°. The system (X_a) is strict.

Then the induced homomorphism of abelian groups $\varprojlim X_a \to \varprojlim Y_b$ is surjective.

Proof. Apply the procedure of (3.2.D) to the morphism of projective systems f. Because of 1°) and 2°) we so obtain an isomorphic morphism of projective systems $(X_t) \to (Y_t)$ such that $X_t \to Y_t$ is surjective for all t; now apply lemma (3.3.A).

q.e.d.

4. SOME ALGEBRAIC GEOMETRY

Notation. CG_k is the category of commutative abelian group schemes over a perfect base field k; CQG_k the category of commutative quasi-algebraic groups over k. In the following we shall mainly work in the category CQG_k and its pro-category; i.e. we shall consider commutative algebraic group schemes up to purely inseparable isogenies. There is a natural (forgetful) functor $CG_k \to CQG_k$ (or, if one prefers, CQG_k is the quotient category of CG_k obtained by equating all infinitesimal groups with the zero group.)
Let $G \in CQG_k$, $G' \in CG_k$ an object which represents G; we define the points of G with values in an algebraic extension l of the base field k as: $G(l) := G'(l)$. Because l is perfect it does not matter which G' is chosen. Section (4.1) lists some properties of the category $Pro(CQG_k)$. In section (4.2) we summarize the Greenberg constructions, which are applied to the group U(K) of units of a local field K in (4.3). In (4.4) we construct the maximal constant quotient of a (pro-)finite commutative quasi-algebraic group. (4.5) contains the definition of the homotopy functors π_0, π_1, $\mathfrak{P}$, of which some properties are given in (4.6).
It is possible to develop the theory of chapter II (for which this section contains some preliminary material) without mentioning quasi-algebraic groups (i.e. one then works exclusively in the categories CG_k and $Pro(CG_k)$). This is done in [10].

(4.1) Some properties of CQG_k and its pro-category.

The category CG_k has finite (fibre) products, it is abelian and all its objects are artinian. (Cf. [SGAD] Exp. V Th. p. 29). It follows that the same holds for the category CQG_k. The pro-category $Pro(CQG_k)$ is therefore abelian (3.2.E),

has arbitrary products, projective limits exist and they are exact ((3.2.G) and (3.2.H)). It follows that $\mathrm{Pro}(\mathrm{CQG}_k)$ satisfies Grothendieck's axiom AB5* (cf. [8] (1.5)). (Let B be a subobject of G, A_i, $i \in I$ a decreasing family of subobjects of G; let $f: G \to G/B$ be the natural projection. Consider the map of projective systems $A_i \to f(A_i)$; it follows from the exactness of the projective limits that $f(\cap A_i) = \cap f(A_i)$ and that $B + \cap A_i = \cap(B + A_i)$, which is AB5* (cf. [GP] p. 19).) Moreover we can select from the objects of CQG_k a *set* $\mathcal{C}$ of cogenerators (i.e. every object of $\mathrm{Pro}(\mathrm{CQG}_k)$ is isomorphic to a subobject of a product of objects of $\mathcal{C}$). It follows that the category $\mathrm{Pro}(\mathrm{CQG}_k)$ has enough projectives ([8] Th. (1.10.1)).
A sequence $0 \to G' \to G \to G'' \to 0$ in $\mathrm{Pro}(\mathrm{CQG}_k)$ is exact iff its sequence of k_s-points $0 \to G'(k_s) \to G(k_s) \to G''(k_s) \to 0$ is exact (cf. [GP] § 1 and (3.3.A) Remark). (If $X := (X_a)$, then $X(k_s) := \varprojlim X_a(k_s)$, in conformity with the general definition of morphisms between pro-objects (cf. (3.2.A)).

(4.2) **The Greenberg construction.** (Cf. [6]; [CAC]).

In this section no proofs are given; they can be found in either of the two references given above.

Let W_n be the ringscheme over k defined by $W_n := \mathrm{Spec}(k[X_0, \ldots, X_{n-1}])$ with the addition and the multiplication defined by the maps $X_i \mapsto S_i$ and $X_i \mapsto P_i$ respectively, where S_i and P_i are the polynomials (in $X_0, \ldots, X_i; Y_0, \ldots, Y_i$) which define the Witt addition and multiplication. (Cf. [CL] Ch. II § 6; the S_i (resp. P_i) satisfy the relations $w_i(S_0, \ldots, S_i) = w_i(X) + w_i(Y)$ (resp. $w_i(P_0, \ldots, P_i) = w_i(X) \cdot w_i(Y)$), where $w_i(X)$ is short for $w_i(X_0, \ldots, X_i) := X_0^{p^i} + pX_1^{p^{i-1}} + \ldots + p^i X_i$; it follows from these relations that the S_i and P_i have integer coefficients.) Then $W_n(B)$, the set of points of the scheme W_n with values in B, is the ring of Witt-vectors of length n over B for any k-algebra B. Let E be a finitely generated module over $W_n(k)$, then E is isomorphic to a direct product $E \simeq W_{n_1}(k) \times W_{n_2}(k) \times \ldots \times W_{n_r}(k)$ for some $n_1, n_2, \ldots, n_r \leqslant n$. (For, as k is perfect, $W_n(k)$ is a principal ideal domain, and its possible quotients are the $W_m(k)$, $m \leqslant n$).
Now assign to E the scheme

$$\mathrm{Sch}(E) := W_{n_1} \times \ldots \times W_{n_r}$$

We then have:

(4.2.1) $\quad \mathrm{Sch}(E)(k) \simeq E \qquad \mathrm{Sch}(E)(k_s) \simeq E \otimes_{W_n(k)} W_n(k_s)$.

Moreover to every $W_n(k)$-multilinear map $f: E_1 \times \ldots \times E_t \to E$ one can assign a morphism of schemes $\mathrm{Sch}(f)$ such that

(4.2.2) $\qquad \mathrm{Sch}(f)(k) \simeq f \qquad \mathrm{Sch}(f)(k_s) \simeq f \otimes_{W_n(k)} W_n(k_s)$.

The functor Sch is, up to purely inseparable isogenies, uniquely determined by these requirements. It has in addition the following property:

(4.2.3) $\qquad$ If $f: E_1 \to E$ is surjective, then $\mathrm{Sch}(f)$ is epimorphic.

Now let A be an artinian local ring with k as residue field, then A is a finitely generated $W_n(k)$-module for some n, and is also a $W_n(k)$-algebra. Addition and multiplication are bilinear, hence we get a structure of ringscheme on Sch(A). The reduction map $s: A \to k$ induces a morphism $s: \mathrm{Sch}(A) \to G_a = \mathrm{Sch}(k)$ (= the additive group over k). Also the canonical lifting map $r: k \to A$ (defined by the requirements: r is a homomorphism such that $s \circ r = \mathrm{id}$. in the case $\mathrm{char}(k) = 0$; and by $s \circ r = \mathrm{id}$. and $r(x^p) = r(x)^p$ for all $x \in k$ in the case $\mathrm{char}(k) = p$) defines a morphism of the corresponding schemes, which is an embedding of G_a onto a closed subscheme of Sch(A).
Let U be the subscheme of units of Sch(A) (cf. [7] section 6). Then we have for U:

(4.2.4) $\qquad$ U is an open multiplicative group subscheme of Sch(A).

$$U(k) = \text{units of } A, \qquad U(k_s) = \text{units of } A \otimes W_n(k_s).$$

The morphism $r: G_a \to \mathrm{Sch}(A)$ embeds G_m homomorphically into U. We have

(4.2.5) $\qquad U \simeq G_m \times U^1$ (as group schemes; $U^1 := \mathrm{Ker}(s: U \to G_m)$)
$\qquad\qquad U^1$ is a unipotent group scheme.

(4.2.6) U is connected and reduced.

Lastly, we remark that:

(4.2.7) If A is free over $W_n(k)$, then Sch(A) represents the functor:

$$B \mapsto A \otimes_{W_n(k)} W_n(B) \qquad (B \text{ a k-algebra}).$$

(Because, as a module over $W_n(k)$, $A \simeq W_n(k)^t$, therefore $\mathrm{Sch}(A) \simeq W_n^t$, $\mathrm{Hom}(\mathrm{Spec}(B), W_n^t) \simeq (\mathrm{Hom}(\mathrm{Spec}(B), W_n))^t \simeq W_n(B)^t \simeq (W_n(k) \otimes_{W_n(k)} W_n(B))^t \simeq$
$\simeq W_n(k)^t \otimes_{W_n(k)} W_n(B) \simeq A \otimes_{W_n(k)} W_n(B)$.)

(4.3) **Pro-algebraic structure on U(K).**

As in section (4.2) almost no proofs are given; they can be found in [CAC] § 1. We shall use the same symbol to denote an object of CG_k and the object of CQG_k which it represents.

Let K be a local field with perfect residue field k. The ring $A_n := A(K)/\mathfrak{m}^n(K)$ is a local artin ring with residue field k. ($\mathfrak{m}^n(K) = 1 + \pi_K^n A(K)$). By applying the constructions of (4.2) one obtains a group scheme $U_n \in CG_k$ such that:

$$(4.3.1) \qquad U_n(k) \simeq U(A(K)/\mathfrak{m}^n(K)) \simeq U(K)/U^n(K)$$
$$U_n(k_s) \simeq U(K_{nr})/U^n(K_{nr}) \simeq U(\hat{K}_{nr})/U^n(\hat{K}_{nr}).$$

If $n > m$, the natural map $A_n \to A_m$ is surjective, and it is $W_t(k)$-linear for some large t. Applying (4.2) again we obtain epimorphisms $Sch(A_n) \to Sch(A_m)$ and $U_n \to U_m$, which on k-points and k_s-points are the usual reductions. Let $U_K \in Pro(CG_k)$ be the pro-algebraic group scheme $U_k := (U_n)_{n \in \mathbf{N}}$ then we have:

$$(4.3.2) \qquad U_K(k) \simeq U(K), \qquad U_K(k_s) \simeq U(\hat{K}_{nr}).$$

U_K has a filtration by sub-group schemes $U_K \supset U_K^1 \supset \ldots \supset U_K^n \supset \ldots$ which is separated ($U_K^n := \mathrm{Ker}(U_K \to U_n)$), and we have:

$$(4.3.3) \qquad U_K^n(k) \simeq 1 + \pi_K^n A(K) = U^n(K),$$
$$U_K^n(k_s) \simeq 1 + \pi_K^n A(\hat{K}_{nr}) = U^n(\hat{K}_{nr}).$$

From (4.2.5) results that:

$$(4.3.4) \qquad U_K \simeq G_m \times U_K^1$$

The morphism $G_a \to U_K^n/K_K^{n+1}$ defined by $x \mapsto 1 + \pi_K^n x$ ($n \geqslant 1$) is a purely inseparable isogeny (of degree $\left[\frac{n}{e}\right]$). It follows that:

$$(4.3.5) \qquad U_K^n/U_K^{n+1} \simeq G_a \quad \text{in } Pro(CQG_k), \quad n \geqslant 1.$$

where the isomorphism on k_s-points is the usual one ($1 + \pi_K^n x \mapsto \bar{x}$). Define an object of $Pro(CQG_k)$ to be connected if it is given by a projective system consisting of connected quasi-algebraic groups. Then we have:

(4.3.6) The pro-quasi-algebraic groups U_K^n are absolutely connected; i.e. $\pi_K^n \otimes_k k_s \simeq U_{\hat{K}_{nr}}^n$ is connected.

(4.4) Maximal constant quotients.

(4.4.A) CONSTANT ALGEBRAIC GROUP SCHEMES.

Let S be an abstract finite group. Consider the ring Map(S,k) of all maps of S into k (pointwise multiplication and addition). The multiplication of the group $S \times S \to S$ induces a co-multiplication $\mathrm{Map}(S,k) \to \mathrm{Map}(S,k) \otimes \mathrm{Map}(S,k)$. We define the *constant algebraic group scheme over* k *belonging to* S as the group scheme $S_k := \mathrm{Spec}(\mathrm{Map}(S,k))$, with the multiplication induced by the co-multiplication described above. If B is any k-algebra without zero divisors, then we have $S_k(B) \simeq \mathrm{Hom}_{\mathrm{Alg}}(\mathrm{Map}(S,k),B) \simeq S$ (whence the name constant group scheme).
The correspondences $S \mapsto S_k$, $G \mapsto G(k_s)$ define an equivalence of categories between the constant algebraic group schemes and the finite abstract groups.

(4.4.B) *Lemma.*

> A finite reduced algebraic group scheme over k is constant iff $G(k) = G(k_s)$. (k is assumed to be perfect).

Proof. It is clear that $G(k) = G(k_s)$ for a constant group scheme G. Conversely, the algebra A of a finite reduced algebraic group scheme G is a reduced artin algebra and therefore $A \simeq \prod_i k_i$, where the k_i are finite (separable, as k is perfect), extensions of k. The k_s-points of G are the maps $A \xrightarrow{p_i} k_i \xrightarrow{\sigma} k_s$ where p_i is the projection on the i-th factor and $\sigma \in G(k, k_i \to k_s)$. Such a point is in G(k) iff it factorizes through k; i.e. iff $k_i = k$ for the index i in question. Therefore $G(k) = G(k_s)$ implies $k_i = k$ for all i, and G is constant.

q.e.d.

(4.4.C) *Lemma.*

> Let G be a finite commutative quasi-algebraic group (or a reduced finite algebraic group scheme), and suppose that H_1 and H_2 are two constant quotients of G. Then there exists a constant quotient H of G larger than both H_1 and H_2.

Proof. Let K_1 and K_2 be the kernels of $G \to H_1$ and $G \to H_2$ respectively. Let $H := G/K_1 \cap K_2$. As H is reduced if G is, we only have to show that $H(k_s)$ is invariant under the action of the galoisgroup $G(k_s/k)$, i.e. that every coset of

$(K_1 \cap K_2)(k_s)$ in $G(k_s)$ is mapped in itself under $G(k_s/k)$. We know that this is the case for the cosets of $K_1(k_s)$ and $K_2(k_s)$. Now $x(K_1(k_s) \cap K_2(k_s)) = xK_1(k_s) \cap xK_2(k_s)$ and we are through.

q.e.d.

(4.4.D) CONSTRUCTION OF THE FUNCTOR Q.

It results from lemma (4.4.C) above and the fact that an abelian finite quasi-algebraic group is artinian (i.e. satisfies the descending chain condition on subgroups) that there exists a maximal constant quotient $Q(G)$ of a finite abelian quasi-algebraic group G. Every homomorphism of G into a constant quasi-algebraic group factorizes uniquely through $Q(G)$. It follows that the functor Q is left adjoint to the inclusion functor I of the category $CCQG_k$ of commutative constant quasi-algebraic groups into the category $FCQG_k$ of finite commutative quasi-algebraic groups,

$$CCQG_k(Q(G), C) \simeq FCQG_k(G, I(C)),$$

it follows that Q is rightexact (cf. [5] Prop. 7 Ch. 1). The category $CCQG_k$ is equivalent to the category FAb of finite abelian groups. Therefore we can extend Q to a functor from the category $Pro(CQG_k)$ into the category of pro-algebraic constant groups, and this extension is also right exact, as is the composed functor $G \mapsto Q(G) \mapsto Q(G)(k_s)$ (3.2.F).

(4.5) The functors π_0, π_1 and $\mathfrak{p}$.

(4.5.A) DEFINITION OF THE FUNCTORS π_0, π_1, $\mathfrak{p}$.

Let $U \in CQG_k$ be a quasi-algebraic group; U° the connected component of the identity of U. We define the functor $\pi_0 : CQG_k \to FCQG_k$ as

(4.5.A.1) $$\pi_0(U) := U/U^\circ$$

π_0 also denotes the canonical extension of this functor to a functor between the pro-categories $Pro(CQG_k)$ and $Pro(FCQG_k)$ (i.e. $\pi_0((U_a)) := (\pi_0(U_a))$. The functors π_i are the left derived functors of π_0. The properties of $Pro(CQG_k)$ mentioned in (4.1) ensure the existence of the π_i. If $0 \to U' \to U \to U'' \to 0$ is an exact sequence in $Pro(CQG_k)$, we have a long exact sequence

(4.5.A.2)
$$\cdots \to \pi_1(U') \to \pi_1(U) \to \pi_1(U'') \to \pi_0(U') \to \pi_0(U) \to \pi_0(U'') \to 0.$$

There is also an explicit description of $\pi_1(U)$ for a connected (pro-)quasi-algebraic group U. Consider all isogenies $0 \to N_f \to U_f \xrightarrow{f} U \to 0$ of U. Another isogeny $0 \to N_g \to U_g \xrightarrow{g} U \to 0$ is said to be larger than f, if there exists a morphism h: $U_g \to U_f$ such that $f \circ h = g$. Such an h induces a morphism $N_g \to N_f$. The finite quasi-algebraic groups N_f with these morphisms form a projective system. It turns out that (cf. [GP] (6.4)):

(4.5.A.3) $$\pi_1(U) \simeq (N_f)_f$$

If we take instead of all isogenies of U only those which have a constant kernel (i.e. $N_f(k_s) = N_f(k)$; cf. (4.4)) we obtain another functor

(4.5.A.4) $$\tau(U) = (N_f)_f, \qquad N_f \text{ constant.}$$

(4.5.B) *Remarks.*

1. For both $\pi_1(U)$ and $\tau(U)$ of a connected quasi-algebraic group U we need sider only those isogenies $0 \to N_f \to U_f \to U \to 0$ for which U_f is connected. Then the factorizing maps $U_g \to U_f$ are all epimorphic, and we find that $\pi_1(U)$ and $\tau(U)$ can be given as strict projective systems.
2. It follows immediately from the definition of the functor Q in (4.4.B) that for a connected quasi-algebraic group $U \in \mathrm{Pro}(CQG_k)$

   (4.5.B.1) $$Q\pi_1(U) \simeq \tau(U)$$

   One can of course use this formula to define $\tau(U)$ also for not necessarily connected quasi-algebraic groups U.
3. If $0 \to U' \to U \to U'' \to 0$ is an exact sequence in $\mathrm{Pro}(CQG_k)$, and U' is connected we have an exact sequence

   $$\pi_1(U') \to \pi_1(U) \to \pi_1(U'') \to 0$$

   and therefore because Q is right exact (4.4.B) exact sequences:

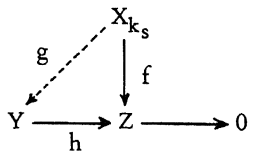
   $$\tau(U') \to \tau(U) \to \tau(U'') \to 0,$$

   $$\tau(U')(k_s) \to \tau(U)(k_s) \to \tau(U'')(k_s) \to 0.$$

(4.5.C) *Lemma.*

Let $X \in \mathrm{Pro}(CG_k)$ be a projective pro-algebraic group scheme over k. Its extension $X_{k_s} \in \mathrm{Pro}(CG_{k_s})$ is then also projective.

Proof. We need only prove that if we have an exact diagram



where Y, Z are algebraic group schemes over k_s, and h is epimorphic, then there exists a morphism g: $X_{k_s} \to Y$ such that $f = h \circ g$. (Cf. (3.2) or [GP] (3.1) Prop. 2). The group schemes Y, Z are algebraic and therefore already defined over a finite extension l of k, which we can assume to be galois. Let $G := G(l/k)$ be the galois group. It suffices to prove that the map $\mathrm{Pro}(CG_l)(X_l, Y) \to \mathrm{Pro}(CG_l)(X_l, Z)$, induced by h is surjective. Quite generally if l/k is a finite extension there exists a functor WR: $CG_l \to CG_k$, the Weil restriction functor, which is right adjoint to the base change functor, i.e. there is a bi-functor isomorphism

$$CG_l(A_l, B) \xrightarrow{\sim} CG_k(A, WR(B)).$$

When l/k is galois, one can describe WR as follows. Let $B \in CG_l$, take the product $B' = \prod_{t \in G} B_t$ of all the conjugates of B, where B_t has the structural morphism $B_t \xrightarrow{t^{-1}} B \to \mathrm{Spec}(l) \xrightarrow{t} \mathrm{Spec}(l)$. There is a natural action of G on B' given on C-points (C an l-algebra) by the formula

$$s((a_t)_{t \in G}) = (b_t)_{t \in G}, \qquad b_t = sa_{s^{-1}t}.$$

This action commutes with the structural morphism $B' \to \mathrm{Spec}(l)$. Therefore there exists a unique scheme WR(B) over k such that $B' \simeq WR(B) \otimes_k l$ and such that the action $t \mapsto WR(B) \otimes_t t$ of G on B' is exactly the above described action. Note that $WR(B) \to WR(A)$ is epimorphic if $B \to A$ is epimorphic. We have a commutative diagram:

$$\begin{array}{ccc} \mathrm{Pro}(CG_l)(X_l, Y) & \to & \mathrm{Pro}(CG_l)(X_l, Z) \\ \wr\| & & \wr\| \\ \mathrm{Pro}(CG_k)(X, WR(Y)) & \to & \mathrm{Pro}(CG_k)(X, WR(Z)) \end{array}$$

The bottom map is surjective because $WR(Y) \to WR(Z)$ is epimorphic and X is projective. It follows that the top map is also surjective.

q.e.d.

Remarks.

1. It is not necessary for the lemma above to suppose that k is perfect.
2. The Weil restriction functor exists more generally as a functor WR: $\mathrm{Sch}_{/l} \to \mathrm{Sch}_{/k}$. Cf. [21]; see also [15] p. 3, 4 for some more remarks on the existence of adjoint functors to the base change functor.
3. For some more information about the conditions under which the image S(P) of a projective object P in an adjoint situation S, T is again projective, cf. [13] Ch. V Th. (7.2).

(4.5.D) *Proposition.*

The functors π_i commute with the base change $k - k_s$.

Proof. The functor π_0 commutes with the base change ([SGAD] Exp. VI_A p. 10). Let $U \in \mathrm{Pro}(\mathrm{CQG}_k)$ be a pro-quasi-algebraic group over k; $\mathbf{X} \to U$ a projective resolution of U over k. We then have:

$$(\pi_i(U))_{k_s} := (H_i(\pi_0(\mathbf{X})))_{k_s} \overset{(1)}{\simeq} H_i(\pi_0(\mathbf{X})_{k_s}) \overset{(2)}{\simeq} H_i(\pi_0(\mathbf{X}_{k_s})) \overset{(3)}{\simeq} \pi_i(U_{k_s}),$$

because of the reasons:
(1) the base change functor $k - k_s$ is exact.
(2) π_0 commutes with the base change $k - k_s$.
(3) $\mathbf{X}_{k_s}$ is a projective resolution of U_{k_s}, because the $(X_i)_{k_s}$ are projective (4.5.C) and because the base change functor $k - k_s$ is exact.

q.e.d.

(4.6) **Some properties of π_1 and π.**

If M is a finite abelian group, $M_l = \{x \in M \mid \mathrm{order}(x) \text{ is a power of } l\}$ denotes the l-primary part of M for every prime number l. We have $M \simeq \prod_l M_l$. If $M = \varprojlim (M_a)$ we define $M_l := \varprojlim (M_a)_l$; we still have $M \simeq \prod_l M_l$.

(4.6.A) *Proposition.*

If $l \neq \mathrm{char}(k)$, then $\pi(U)(k_s) = 0 = \pi_1(U)(k_s)$ for unipotent pro-quasi-algebraic groups U over k.

Proof. Multiplication with l is an isomorphism $U \to U$; therefore $\pi_1(U)(k_s) \overset{l}{\to}$

$\pi_1(U)(k_s)$ is also an isomorphism, which proves that $\pi_1(U)(k_s) = 0$. The pro-quasi-algebraic group $\mathfrak{r}(U)$ is a quotient of $\pi_1(U)$.

q.e.d.

(4.6.B) *Proposition.*

$$\mathfrak{r}(G_m)(k_s) = \mathfrak{r}(G_m)(k) \simeq \mu(K) := \text{group of all roots of unity of } k.$$

Proof. We know that over k_s the maps $G_m \xrightarrow{n} G_m$ are cofinal in the system of all isogenies of G_m (cf. [GP] § 6 Prop. 9). Now let $0 \to N \to E \xrightarrow{f} G_m \to 0$ be an isogeny with constant kernel. According to the above there exist a natural number n and a morphism $g: G_m \to E$ defined over k_s which factorizes n through f. Let $s \in G(k_s/k)$, then $f(s^{-1}gs-g) = s^{-1}ns-n = 0$; i.e. $s^{-1}gs-g$ factorizes through N. But G_m is connected and N is finite, so we have $s^{-1}gs-g = 0$; i.e. g is defined over k. Taking the image of G_m under g in E we obtain an isogeny of type $G_m \xrightarrow{n'} G_m$ with constant kernel, which is larger than the f we started with. An isogeny $G_m \xrightarrow{r} G_m$ has constant kernel iff k contains the r-th roots of unity.

q.e.d.

(4.6.C) *Proposition.*

Let $G \in CQG_k$ be a connected commutative quasi-algebraic group. Then

$$\mathrm{Hom}(\mathfrak{r}(G), (\mathbf{Z}/p\mathbf{Z})_k) \simeq \mathrm{Ext}(G, (\mathbf{Z}/p\mathbf{Z})_k).$$

Proof. Let $\bar{G} := (G_f)$, where $G_f \xrightarrow{f} G$ runs through all connected isogenies of G. Then we have by definition of π_1 an exact sequence

$$0 \to \pi_1(G) \to \bar{G} \to G \to 0.$$

Now $\mathrm{Ext}(N, \bar{G}) = 0$ if N is a finite group. For let $0 \to N \to X \to \bar{G} \to 0$ be an extension of $\bar{G}$; then there is an G_f such that this extension is obtained from an extension $0 \to N \to X_f \to G_f \to 0$ (because N is finite; cf. [GP] (3.4) Prop. 7). But $X_f \to G_f \to G$ is an isogeny of G, hence $\bar{G} \to G$ factorizes through X_f. The morphism $\bar{G} \to X_f$ defines a section of the extension $0 \to N \to X \to \bar{G} \to 0$. Consider part of the long exact sequence of the Hom and Ext groups

$$\mathrm{Hom}(\bar{G}, (\mathbf{Z}/p\mathbf{Z})_k) \to \mathrm{Hom}(\pi_1(G), (\mathbf{Z}/p\mathbf{Z})_k) \to \mathrm{Ext}(G, (\mathbf{Z}/p\mathbf{Z})_k) \to \mathrm{Ext}(\bar{G}, (\mathbf{Z}/p\mathbf{Z})_k)$$

Now $\mathrm{Hom}(\bar{G}, (\mathbf{Z}/p\mathbf{Z})_k) = 0$ because $\bar{G}$ is connected and $(\mathbf{Z}/p\mathbf{Z})_k$ is finite; by the

above $\mathrm{Ext}(\bar{G},(\mathbf{Z}/p\mathbf{Z})_k) = 0$; therefore we have an isomorphism

$$\mathrm{Hom}(\pi_1(G), (\mathbf{Z}/p\mathbf{Z})_k) \xrightarrow{\sim} \mathrm{Ext}(G, (\mathbf{Z}/p\mathbf{Z})_k)$$

But $(\mathbf{Z}/p\mathbf{Z})_k$ is constant. By the definition of the functor Q every homomorphism $\pi_1(G) \to (\mathbf{Z}/p\mathbf{Z})_k$ factors uniquely through $Q\pi_1(G) \simeq \mathfrak{T}(G)$ (cf. (4.4.D), (4.5.B)).

q.e.d.

(4.6.D) ISOGENITIES OF G_a OVER K_s.

Suppose $\mathrm{char}(k) = p \neq 0$. All non-trivial isogenies of G_a with kernel $(\mathbf{Z}/p\mathbf{Z})_k$ over k_s are of the type

$$0 \to (\mathbf{Z}/p\mathbf{Z})_k \xrightarrow{f} G_a \xrightarrow{g} G_a \to 0$$

where f is multiplication with an element $c \in k_s$, and g is given by $g(x) = ax^p + bx$, where $a, b, c \in k_s$ are such that $ab \neq 0$, $ac^p + bc = 0$. Two of these extensions are isomorphic iff the numbers $a^{-1}c^{-p}$ are equal. ([GP] § 8 Prop. 3). The map $(0 \to (\mathbf{Z}/p\mathbf{Z})_k \xrightarrow{f} G_a \xrightarrow{g} G_a \to 0) \mapsto a^{-1}c^{-p}$ defines an isomorphism

$$\mathrm{Ext}(G_a, (\mathbf{Z}/p\mathbf{Z})_k) \xrightarrow{\sim} k_s$$

(4.6.E) FORMS OF AN ALGEBRAIC GROUP.

Let U be an algebraic group over k, and l/k a (galois) extension of k. An algebraic group U' over k is called an l/k-form of U iff $U_l \simeq U'_l$. The group $G(l/k) = G$ acts on the automorphism group $A(U_l)$ of l-automorphisms of U_l as $s(\varphi) = s\varphi s^{-1}, s \in G, \varphi \in A(U_l)$.

Proposition. There is a 1–1 correspondence between the set $E_{l/k}(U)$ of l/k-forms of an algebraic group U, and the cohomology group $H^1(G(l/k), A(U_l))$ (k is assumed to be perfect).

For a proof cf. [18] Ch. III § 1.

(4.6.F) *Application.*

The algebraic group G_a has no other l/k-forms than itself for all galois extensions l/k.

Proof. An automorphism $(G_a)_l \to (G_a)_l$ is given by an algebra homomorphism $l[X] \to l[X]$, $X \mapsto f(X)$; there must be an inverse automorphism; this shows that degree $f(X)) = 1$. The morphism $(G_a)_l \to (G_a)_l$ must be additive, which implies that for $f(X)$ we must have $f(1 \otimes X + X \otimes 1) = 1 \otimes f(X) + f(X) \otimes 1$ which shows that $f(X) = uX$ for some non zero constant $u \in l$. The action of $G\,l/k)$ on $A((G_a)_l)$ becomes the galois action under this identification. But $\hat{H}^1(G(l/k),l^*)=0$ by (1.7) ("Hilbert 90"). An application of (4.6.E) concludes the proof.

q.e.d.

Remark. (4.6.F) is no longer necessarily true if l/k is non-separable.

(4.6.G) *Proposition.*

If $\mathrm{char}(k) = p$, then $\mathrm{Hom}_k(\pi(G_a), (\mathbf{Z}/p\mathbf{Z})_k) \simeq k$.

Proof. The algebraic group G_a has no other k_s/k-forms than itself. (k is perfect!). Therefore according to (4.6.D) above, if we have a nontrivial extension $0 \to (\mathbf{Z}/p\mathbf{Z})_k \to X \to G_a \to 0$ then $X \simeq G_a$ and we have an extension of the type $0 \to (\mathbf{Z}/p\mathbf{Z})_k \xrightarrow{f} G_a \xrightarrow{g} G_a \to 0$ where f is given by $1 \mapsto c$, g by $x \mapsto ax^p + bx$, with the relations $ab \neq 0$ and $ac^p + bc = 0$ between $a, b, c \in k_s$. The morphism f is defined over k iff $c \in k$, and g is defined over k iff $a, b \in k$. Therefore we have an isomorphism $\mathrm{Ext}(G_a,(\mathbf{Z}/p\mathbf{Z})_k) \simeq k$ (4.6.D), and we are through in view of (4.6.C).

q.e.d.

(4.7) **Lemma on short exact sequences.**

Let $o \to N \to X \to U \to 0$ and $o \to N' \to X' \to U \to 0$ be two short exact sequences (in $\mathrm{Pro}(CG_k)$ or in $\mathrm{Pro}(CQG_k)$) with X, X' connected and N, N' pro-finite. Suppose that there exists a morphism $f'\colon X_{k_s} \to X'_{k_s}$ with an exact diagram

$$\begin{array}{ccccccc} o & \to & N_{k_s} & \to & X_{k_s} & \to & U_{k_s} \to 0 \\ & & \downarrow & & \downarrow f' & & \| \\ o & \to & N'_{k_s} & \to & X'_{k_s} & \to & U_{k_s} \to 0 \end{array}$$

then there exists a morphism $f\colon X \to X'$ with an exact diagram

$$\begin{array}{ccccccccc} o & \to & N & \to & X & \to & U & \to & 0 \\ & & \downarrow f & & \downarrow f & & \| & & \\ o & \to & N' & \to & X' & \to & U & \to & 0 \end{array}$$

such that $f_{k_s} = f'$. The morphism f is an isomorphism iff f' is an isomorphism.

Proof. We only have to show that f' commutes with the action of $G(k_s/k)$ on X_{k_s} and X'_{k_s}. Let $s \in G(k_s/k)$; composing $s^{-1}f's - f'$ with $X'_{k_s} \to U_{k_s}$ gives zero, accordingly $s^{-1}f's - f'$ factorizes through N'_{k_s}; but X_{k_s} is connected (because X is) and N'_{k_s} is pro-finite; it follows that $s^{-1}f's - f' = 0$.

q.e.d.

CHAPTER II

MAXIMAL ABELIAN EXTENSIONS OF LOCAL FIELDS

This chapter delas with a description of the galois group $\mathfrak{Gl}_K$ (defined in (2.8.H), cf. also (2.8.J)) in terms of isogenies of the pro-quasi-algebraic group U_K ('of units of K'; K is a local field with perfect residue field k). In [CAC] Serre proved that $\pi_1(U_K) \simeq \mathfrak{Gl}_K$ when k is algebraically closed. In this chapter we generalize Serre's theorem to $\mathfrak{P}(U_K)(k) \simeq \mathfrak{Gl}_K$ where $\mathfrak{P}(U_K)$ is the maximal constant quotient of $\pi_1(U_K)$. (Cf. (4.5.B) and (4.4.D)).
Let L/K be a galois extension. The galoisgroup $G(L_{nr}/K)$ acts continuously on L_{nr}, hence we can extend this action by continuity to an action on $\hat{L}_{nr}$. (Note that the K-automorphisms of $\hat{L}_{nr}$ so obtained are exactly the continuous K-automorphisms of $\hat{L}_{nr}$).

5. **STATEMENT OF THE THEOREM** (5.4.D).

In this section we define a surjective homomorphism $\vartheta: \mathfrak{P}(U_K)(k_s) \to \mathfrak{Gl}_K$, which will be proved to be an isomorphism in section 6, and again in section 7.
Section (5.1) contains some lemmas on the action of $G(k_s/k)$ on $U_K(k_s)$.
In (5.2) we encounter the algebraic geometric version of the fundamental exact sequence (2.7.A.2); (5.3) is a lemma on the functoriality of this sequence.
Section 5 closes with (5.4) wherein we define the homomorphism ϑ: $\mathfrak{P}(U_K)(k_s) \to \mathfrak{Gl}_K$ and show that it is surjective.

(5.1) **The action of** $G(k_s/k)$ **on** $U_K(k_s)$.

Let K be a local field with perfect residue field k; $\hat{K}_{nr}$ denotes the completion of the maximal unramified extension K_{nr} of K. According to (4.3) there exists a pro-quasi-algebraic group U_K such that $U_K(k) \simeq U(K)$ and $U_K(k_s) \simeq U(\hat{K}_{nr})$.
There are two natural actions of $G(k_s/k)$ on $U_K(k_s)$:

1° the action defined by the pro-quasi-algebraic group structure of U_K over k.

2° let φ be the canonical homomorphism which lifts $G(k_s/k)$ to $G(K_{nr}/K)$ (see e.g. [22] Prop 3-5-1) and define $s(u) := \varphi(s)(u)$ for $s \in G(k_s/k)$, $u \in U(\hat{K}_{nr}) \subset \hat{K}_{nr}$.

(5.1.A) *Lemma*

These two actions coincide.

Proof. Both actions can be extended to an action on $A(\hat{K}_{nr})$ as a group of continuous ring automorphisms which leave $A(K)$ pointwise invariant and both reduce mod. $\mathfrak{m}(\hat{K}_{nr})$ to the galois action of $G(k_s/k)$ on k_s. There is only one such action of $G(k_s/k)$ on $A(K_{nr}) \subset A(\hat{K}_{nr})$. (Again according to [22] Prop 3-5-1). The lemma follows by continuity.

q.e.d.

(5.1.B) TOTALLY RAMIFIED GALOIS EXTENSIONS.

Let L/K be a totally ramified galois extension. By (2.7.A) we have an exact sequence (2.7.A.2):

$$(5.1.B.1) \qquad 0 \to G(L/K)^{ab} \to U(\hat{L}_{nr})/V(\hat{L}_{nr}) \to U(\hat{K}_{nr}) \to 0.$$

The induced action of $G(k_s/k)$ on $G(L/K)^{ab} = G(\hat{L}_{nr}/\hat{K}_{nr})^{ab}$ is the action by inner automorphisms ((5.1.A) and (2.7.A.3)); i.e. if $\bar{s} \in G(k_s/k)$ and $t \in G(L/K)$ represents $\bar{t} \in G(L/K)^{ab}$, and $s \in G(L_{nr}/K)$ is any lift of $\bar{s}$, then $\bar{s}(\bar{t}) = sts^{-1}$ (as $s\left(\frac{t\pi_L}{\pi_L}\right) = \frac{sts^{-1}(s\pi_L)}{s\pi_L} \equiv \frac{sts^{-1}(\pi_L)}{\pi_L}$).

(5.1.C) *Lemma*

$G(L/K)^{ab}$ is invariant under the action of $G(k_s/k)$ (when L/K is totally ramified galois).

Proof. This follows from the fact that L/K and K_{nr}/K are linearly disjoint and from (5.1.B) above.

q.e.d.

(5.2) **The fundamental exact sequence.**

Let L/K be any finite totally ramified extension. A homomorphism $s \in G(K, L \to \Omega)$ induces a linear morphism s: $A(L) \to A(sL)$, and hence gives rise to a morphism of pro-algebraic schemes s: $U_L \to U_{sL}$. We now define the morphism $N_{L/K}$: $U_L \to U_K$ to be the composite

$$U_L \longrightarrow \prod_s U_{sL} \xrightarrow{\text{mult.}} U_K,$$

$$x \longmapsto (s_1x,\ldots,s_nx) \longmapsto \prod_s sx.$$

(5.2.A) *Lemma.*

Let L/K be a totally ramified galois extension, and let C be the kernel of the morphism $N_{L/K}: U_L \to U_K$. We then have $C^o_{red} = I_G U_L$, (and hence $C^o = I_G U_L$ in the category $Pro(CQG_k)$. (Where $G = G(L/K)$, and C^o_{red} denotes the maximal reduced subscheme of the connected component of the identity C^o of C; C^o_{red} is a pro-algebraic *group* sub-scheme of C (cf. [16] Lemma (1.11))).

Proof. The pro-algebraic group scheme $I_G U_L$ is the sum of the group schemes $(s-1)U_L$ $(s \in G)$ which are all connected and reduced; their intersection is non-empty; therefore $I_G U_L$ is connected and reduced; hence $I_G U_L \subset C^o_{red}$. On the other hand $C(k_s)/I_G U_L(k_s) \simeq G(L/K)^{ab}$ is a finite group (5.1.B.1).

q.e.d.

Remark.

The pro-algebraic group scheme C is in general not reduced. Cf. § 8.

(5.2.B) THE FUNDAMENTAL EXACT SEQUENCE

Let V_L denote the connected component of the identity of the kernel of $N_{L/K}: U_L \to U_K$, where again L/K is supposed to be totally ramified galois. We see then from (5.2.A) that the exact sequence (2.7.A.2) is nothing else but the sequence of k_s-points of the exact sequence of pro-quasi-algebraic groups (or pro-algebraic group schemes)

(5.2.B.1) $$0 \to \mathbf{G}(L/K)^{ab} \to U_L/V_L \to U_K \to 0,$$

where $\mathbf{G}(L/K)^{ab}$ is some form of $(G(L/K)^{ab})_k$. But (5.1.C) now shows that:

(5.2.B.2) $\mathbf{G}(L/K)^{ab}$ is constant; i.e. $\mathbf{G}(L/K)^{ab} \simeq (G(L/K)^{ab})_k$.

(cf. (4.4.B)). The symbol $E_{L/K}$ will denote the element of $Ext(U_K, \mathbf{G}(L/K)^{ab})$ determined by the exact sequence (5.2.B.1).

(5.2.C) DEFINITION OF THE HOMOMORPHISMS $\vartheta_{L/K}$.

From (5.2.A) we see that $\mathbf{G}(L/K)^{ab} \simeq \pi_0(\mathrm{Ker}\, N_{L/K})$; writing down the long exact sequence of $0 \to C \to U_L \to U_K \to 0$ now gives an exact sequence

$$\pi_1(U_L) \to \pi_1(U_L) \to \mathbf{G}(L/K)^{ab} \to 0$$

(for U_L is connected (4.3.6)). The quasi-algebraic group $\mathbf{G}(L/K)^{ab}$ is constant; therefore, taking maximal constant quotients (which is a right exact functor (4.4.D)) we obtain exact sequences

(5.2.C.1) $$\mathfrak{N}(U_L) \to \mathfrak{N}(U_K) \to \mathbf{G}(L/K)^{ab} \to 0$$

(5.2.C.2) $$\mathfrak{N}(U_L)(k_s) \longrightarrow \mathfrak{N}(U_K)(k_s) \xrightarrow{\vartheta_{L/K}} G(L/K)^{ab} \longrightarrow 0$$

The morphism $\mathfrak{N}(U_K) \to \mathbf{G}(L/K)^{ab}$ in the sequence (5.2.C.1) above is the same as the morphism defined by the isogeny (5.2.B.1).

(5.2.D) *Lemma*

Let L/K be any finite totally ramified extension. Then there exists a finite abelian totally ramified extension M/K such that

$$N_{M/K}(\mathfrak{N}(U_M)) \subset N_{L/K}(\mathfrak{N}(U_L)) \subset \mathfrak{N}(U_K).$$

Proof. Let L' be any finite galois extension of K which contains L. Let $G := G(L'/K)$; let K_n be the maximal unramified extension of K contained in L', let $H := G(L'/K_n)$. Let M' be the invariant field of the normal subgroup $\langle H, G\rangle$ of G; as H is normal in G, $\langle H, G\rangle \subset H$. The group $H/\langle H, G\rangle$ is central in $G/\langle H, G\rangle$, therefore, according to (2.8), we can suppose, by enlarging K_n if necessary, that:

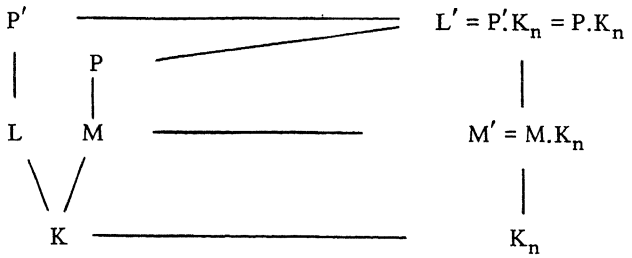
1° there exists a totally ramified abelian extension M/K such that $M \subset L'$ and $M \cdot K_n = M'$, (2.8.F),

2° there exists a totally ramified extension P such that $M \subset P \subset L'$ and $P \cdot K_n = L'$, (2.8.E),

3° there exists a totally ramified extension P' such that $L \subset P' \subset L'$ and $P' \cdot K_n = L'$, (2.8.E).

We have:

(5.2.D.1) $$G(M/K) \simeq H/\langle H, G\rangle.$$



Now let V_P be the connected component of the identity of the kernel of the morphism $N_{P/K}$ from U_P to U_K. This give an exact sequence

$$(5.2.D.2) \qquad 0 \longrightarrow D \longrightarrow U_P/V_P \xrightarrow{N_{P/K}} U_K \longrightarrow 0,$$

where D is finite, which after base extension $k \longrightarrow k_n$ (where k_n is the residue field of K_n) becomes isomorphic to the exact sequence

$$0 \to \mathbf{G}(L'/K_n)^{ab} \to U_{L'}/V_{L'} \to U_{K_n} \to 0.$$

It follows that $D(k_s) \simeq H^{ab} = G(L'/K_n)^{ab}$. The action of $G(k_s/k)$ on $D(k_s)$ is, however, not trivial in general; in fact the maximal constant quotient of D is $(H/\langle H,G\rangle)_k$. (Because the action of $G(k_s/k)$ on $H^{ab} \simeq D(k_s)$ is by inner automorphisms, (5.1.B).)

The sequence (5.2.D.2) yields an exact sequence

$$\pi_1(U_P/V_P) \to \pi_1(U_K) \to D \to 0$$

and hence an exact sequence (the functor Q is right exact!)

$$\pi(U_P/V_P) \to \pi(U_K) \to (H/\langle H,G\rangle)_k \to 0,$$

which composed with the epimorphism

$$\pi(U_P) \to \pi(U_P/V_P),$$

gives an exact sequence

$$\pi(U_P) \to \pi(U_K) \to (H/\langle G,H\rangle)_k \to 0.$$

The morphism $\pi(U_P) \to \pi(U_K)$ factorizes through $\pi(U_M)$ (simply because $M \subset P$), and there is also an exact sequence (5.2.C.1)

$$\pi(U_M) \to \pi(U_K) \to \mathbf{G}(M/K) \to 0$$

where $G(M/K) \simeq (G/\langle G,H\rangle)_k$. (5.2.D.1). Hence

(5.2.D.3) $$N_{M/K}(\pi(U_M)) = N_{P/K}(\pi(U_P))$$

The exact sequence $0 \to D \to U_P/V_P \to U_K \to 0$ and the analogous sequence $0 \to D' \to U_{P'}/V_{P'} \to U_K \to 0$ become isomorphic after base extension $k \longrightarrow k_n$ because $P.K_n = P'.K_n = L'$. This yields an exact diagram (4.7)

$$\begin{array}{ccccccc} 0 \to & D & \to & U_P/V_P & \to & U_K & \to 0 \\ & \downarrow & & \downarrow & & \| & \\ 0 \to & D' & \to & U_{P'}/V_{P'} & \to & U_K & \to 0. \end{array}$$

It follows that $N_{P/K}\pi(U_P/V_P) = N_{P'/K}\pi(U_{P'}/V_{P'})$, and, as the natural morphisms $\pi(U_P) \to \pi(U_P/V_P)$, $\pi(U_{P'}) \to \pi(U_{P'}/V_{P'})$ are epimorphic, that

(5.2.D.4) $$N_{P/K}\pi(U_P) = N_{P'/K}\pi(U_{P'}).$$

Now $N_{P'/K}\pi(U_{P'}) \subset N_{L/K}\pi(K_L)$ because $L \subset P'$. Combining this with (5.2.D.3) and (5.2.D.4) yields:

$$N_{M/K}\pi(U_M) = N_{P/K}\pi(U_P) = N_{P'/K}\pi(U_{P'}) \subset N_{L/K}\pi(U_L).$$

q.e.d.

(5.3) **Functoriality.**

Let L/K and M/K be two totally ramified galois extensions such that $L \subset M$, then the following diagrams are commutative

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(M/K)^{ab} & \longrightarrow & U_M/V_M & \xrightarrow{N_{M/K}} & U_K & \longrightarrow & 0 \\ & & \downarrow q & & \downarrow N_{M/L} & & \| & & \\ 0 & \longrightarrow & G(L/K)^{ab} & \longrightarrow & U_L/V_L & \xrightarrow{N_{L/K}} & U_K & \longrightarrow & 0, \end{array}$$

$$\begin{array}{ccccccc} \pi(U_M) & \xrightarrow{N_{M/K}} & \pi(U_K) & \longrightarrow & G(M/K)^{ab} & \longrightarrow & 0 \\ \downarrow N_{M/L} & & \| & & \downarrow q & & \\ \pi(U_L) & \xrightarrow{N_{L/K}} & \pi(U_K) & \longrightarrow & G(L/K)^{ab} & \longrightarrow & 0, \end{array}$$

where q is the natural projection. The commutativity of the left hand square in the first diagram follows from (2.7.A.3) and the fact that $N_{M/L}(\pi_M)$ is a uniformizing element of L if π_M is a uniformizing element of M; the commutativity of the second diagram follows from that of the first. (Cf. (5.2.C)).

(5.4) **Statement of the theorem.**

Let $\mathfrak{A}_K := G(K^{ab}/K)_{ram}$:= the ramified part of the galois group of the maximal abelian extension of K (cf. (2.8.H)).

(5.4.A) *Lemma*

Let L/K and L′/K be two abelian totally ramified extensions such that $L.K_{nr} = L'.K_{nr}$, then also $L.K_{nr}^{ab} = L'.K_{nr}^{ab}$.

Proof. Let K_n be the maximal unramified extension of K contained in L.L′; then $L.K_n = L'.K_n$, and K_n/K is abelian because L.L′/K is abelian.

q.e.d.

(5.4.B) *Lemma*

Let L,L′ be two abelian totally ramified extensions such that $L.K_{nr} = L'.K_{nr}$ then $U_L/V_L \simeq U_{L'}/V_{L'}$ and $E_{L/K} = E_{L'/K}$.

Proof. This follows from (4.7) because of $L.K_{nr} = L'.K_{nr}$.

(5.4.C) DEFINITION OF THE HOMOMORPHISM ϑ.

According to (5.2.B) we have for every totally ramified abelian L/K an isogeny with constant kernel

$$0 \to \mathbf{G}(L/K) \to U_L/V_L \to U_K \to 0.$$

This defines a homomorphism $\vartheta_{L/K} : \pi(U_K)(k_s) \to G(L/K)$, cf. (5.2.C).
If L′/K is another totally ramified extension, then there exists by lemma (5.4.A), the corollary to the pull-back theorem (2.8.G) and lemma (5.4.B) an isogeny

$$0 \to \mathbf{G}(M/K) \to K_M/V_M \to U_K \to 0,$$

which is larger than both $U_{L'}/V_{L'} \to U_K$ and $U_L/V_L \to U_K$, (cf. also (5.3)).

Letting L run through all totally ramified abelian extension and taking projective limits we obtain a homomorphism (cf. (5.3) and (2.8.H)):

(5.4.C.1) $$\vartheta: \pi(U_K)(k) = \pi(U_K)(k_s) \to \mathfrak{A}_K.$$

This homomorphism is surjective for the following reasons.
1° U_L is connected; $\pi(U_K)$ is given by a strict system (cf. (4.5.B)).
2° For every finite quotient G of $\mathfrak{A}$ there exist a totally ramified abelian L/K such that $G \simeq G(L/K)$ (2.8.H).
3° The lemma (3.3.B) on projective limits of finite abelian groups.

(5.4.D) *Theorem*

The surjective homomorphism ϑ above (5.4.D.1) is an isomorphism.

This theorem will be proved in the following section (§ 6).

6. PROOF OF THE THEOREM (5.4.D).

In this section we prove theorem (5.4.D), which states that the homomorphism ϑ is an isomorphism. The proof given here is an adaptation of the proof given by Serre in [CAC] for the algebraically closed case ($k = k_s$).
A brief outline of the proof follows here. We decompose both $\mathfrak{A}_K$ and $\pi(U_K)(k_s)$ in their l-primary parts (cf. (4.6)), as well as the homomorphism ϑ between these groups. It is not difficult to prove that the homomorphisms ϑ_l are isomorphisms when $l \neq p = \mathrm{char}(k)$. This is done in (6.1). After studying some properties of extensions of degree p in (6.2), and after proving some lemmas in (6.3), we give in (6.4) and (6.5) a number of examples of extensions of degree p (all totally ramified). It turns out these consitute sufficiently many extensions of degree p; in the sense that these extensions suffice to show that the dual homomorphism ϑ^*: $\mathrm{Hom}(\mathfrak{A}_K, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{Hom}(\pi(U_K)(k_s), \mathbf{Z}/p\mathbf{Z})$ is surjective (6.6). This fact and lemma (5.2.D) are used to complete the proof of the theorem (5.4.D) in (6.7), except for lemma (6.4) which is only proved for $k = k_s$ in (6.4). Section (6.8) contains the proof of lemma (6.4) when k is not necessarily algebraically closed.

U_K, U_K^1, ... etc. are in this section always taken as objects of the category $\mathrm{Pro}(CQG_k)$ of pro-quasi-algebraic groups over the base field k.

(6.1) **The case** $l \neq p = \mathrm{char}(k)$.

Both $\pi(U_K)(k_s)$ and $\mathfrak{A}_K$ are pro-finite groups, and therefore they decompose as the product of their l-primary parts (l a prime number; cf. (4.6))

$$\pi(U_K)(k_s) \simeq \prod_l (\pi(U_K)(k_s))_l \,, \quad \mathfrak{A}_K \simeq \prod_l (\mathfrak{A}_K)_l,$$

where l runs through all prime numbers. The homomorphism ϑ likewise decomposes as the product of the induced homomorphisms ϑ_l: $\pi(U_K)(k_s)_l \to (\mathfrak{A}_K)_l$ thus it suffices to prove that ϑ_l are isomorphisms.

(6.1.A) *Lemma*

If $l \neq p := \mathrm{char}(k)$, then ϑ_l is an isomorphism.

The pro-quasi-algebraic group U_K decomposes as $U_K \simeq U_K^1 \times G_m$ (4.3.4); whence $\pi(U_K) \simeq \pi(U_K^1) \times \pi(G_m)$;the group U_K^1 is unipotent (cf. (4.3.5)), therefore $\pi(U_K^1)(k_s)_l = 0$ (4.6.A). Furthermore $\pi(G_m)_l = \mu_{l^\infty}(k) :=$ group of all l^n-th roots of unity in k for all n (4.6.B). The homomorphism ϑ_l is surjective (5.4.C). If there exist l^n-th roots of unity in k, then they also exist in K (Hensel's lemma), and the extension of K defined by $X^{l^n} - \pi_K$ is totally ramified abelian and yields an isogeny which is multiplication with l^n on G_m. This concludes the proof in view of (4.6.B)

q.e.d.

The only thing left to prove is that ϑ_p is an isomorphism in the case $p = \mathrm{char}(k) \neq 0$. We therefore assume from now on in this section that $\mathrm{char}(k) \neq 0$.

(6.1.B) DEFINITION OF $H(U_K)$ AND $H(\mathfrak{A}_K)$.

Let U be a pro-quasi-algebraic group over k. We define $H(U) := \mathrm{Ext}(U, \mathbf{Z}/p\mathbf{Z})_k) \simeq \mathrm{Pro}(CQG_k)(\pi(U), (\mathbf{Z}/p\mathbf{Z})_k) \simeq \mathrm{Hom}(\pi(U)(k_s), \mathbf{Z}/p\mathbf{Z})$ (4.6.C). If $f: U \to V$ is a morphism of pro-quasi-algebraic groups, let f^* be the induced homomorphism $H(V) \to H(U)$. In addition we define $H(\mathfrak{A}_K) := \mathrm{Hom}(\mathfrak{A}_K, \mathbf{Z}/p\mathbf{Z})$ and $\vartheta^* = \vartheta_p^* :=$ the homomorphism defined by ϑ:

$$\vartheta^*: \mathrm{Hom}(\mathfrak{A}_K, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{Hom}(\pi(U)(k_s), \mathbf{Z}/p\mathbf{Z}) \simeq \mathrm{Ext}(U, (\mathbf{Z}/p\mathbf{Z})_k).$$

(6.2) **Extensions of degree** p.

(6.2.A) Let $\xi : \mathfrak{A}_K \to \mathbf{Z}/p\mathbf{Z}$ be an element of $H(\mathfrak{A}_K)$. This element defines a

totally ramified abelian extension L/K of degree p (2.8) and a choice of an isomorphism $\mathbf{Z}/p\mathbf{Z} \simeq G(L/K)$ (i.e. a choice of a generator). Then $\vartheta^*(\xi)$ is the element of $H(U_K) \simeq \mathrm{Ext}(U_K, (\mathbf{Z}/p\mathbf{Z})_k)$ represented by the sequence

$$0 \longrightarrow (\mathbf{Z}/p\mathbf{Z})_k \longrightarrow U_L/V_L \xrightarrow{N} U_K \longrightarrow 0$$

((5.2.B.1); same choice of isomorphism $\mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} G(L/K)$).
Let t be the largest integer such that $G_t = G$ (where $G := G(L/K)$; cf. (2.5)); the image of G under the homomorphism $G \xrightarrow{i} U_L(k_s)$ $(s \longmapsto \frac{s\pi_L}{\pi_L})$ is then contained in $U_L{}^t(k_s)$ by the definition of t. We have according to (2.7.B)

(6.2.A.1) $$(\mathrm{Ker}N)(k_s) \cap U_L^{t+1}(k_s) = V_L(k_s)$$

The norm morphism $N: U_L \to U_K$ induces a sequence

(6.2.A.2) $$0 \longrightarrow \mathbf{G} \longrightarrow U_L/U_L^{t+1} \xrightarrow{N'} U_K/U_K^{t+1} \longrightarrow 0$$

because $\psi(t) = t$ (cf. (2.6)); where $\mathbf{G} := \mathbf{G}(L/K) \simeq (G(L/K))_k$.
This sequence (6.2.A.2) is exact, which is proved by some diagram chasing and an application of (2.6.E) in the diagram (6.2.A.3) below.

(6.2.A.3)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & G & \xrightarrow{i} & U_L(k_s)/V_L(k_s) & \xrightarrow{N} & U_K(k_s) & \longrightarrow & 0 \\ & & \| & & \downarrow q & & \downarrow & & \\ 0 & \longrightarrow & G & \xrightarrow{i} & U_L(k_s)/U_L^{t+1}(k_s) & \xrightarrow{N'} & U_K(k_s)/U_K^{t+1}(k_s) & \longrightarrow & 0 \end{array}$$

(We have $i(G) \cap U_L{}^{t+1}(k_s) = \{1\}$ (definition of t; G is cyclic of prime order!), and the homomorphism N' is clearly surjective. Let $x \in U_L(k_s)$ be such that $N'(x) = 0$; then $N(x) \in U_K{}^{t+1}(k_s)$. The homomorphism $N: U_L{}^{t+1}(k_s) \longrightarrow U_K{}^{t+1}(k_s)$ is surjective ((2.6.E); $\psi(t) = t$). Let $y \in U_L{}^{t+1}(k_s)$ be such that $N(x) = N(y)$, then $q(y^{-1}x) = q(x)$ and $N'(y^{-1}x) = 0$, therefore $x \equiv y^{-1}x \in i(G) \bmod U_L{}^{t+1}(k_s)$ which proves the exactness of the lower sequence in the middle.)

(6.2.B) The right hand square in the diagram (6.2.A.3) is cartesian according to (6.2.A.1); i.e. the element of $H(U_K) \simeq \mathrm{Ext}(U_K, \mathbf{G})$ represented by the upper row is the image of the element of $H(U_K/U_K{}^{t+1}) \simeq \mathrm{Ext}(U_K/U_K^{t+1}, \mathbf{G})$ represented by the lower row under the homomorphism induced by the natural projection

$U_K \longrightarrow U_K/U_K{}^{t+1}$.

(6.2.C) Taking the image of $\vartheta^*(\xi) \in H(U_K/U_K{}^{t+1})$ in $H(U_K^t/U_K^{t+1})$ we obtain the element represented by the exact sequence

$$0 \longrightarrow (\mathbf{Z}/p\mathbf{Z})_k \xrightarrow{\gamma} U_L^t/U_L^{t+1} \xrightarrow{N_t} U_K^t/U_K^{t+1} \longrightarrow 0$$

where N_t is induced by the norm morphism (cf. (2.6)) and γ is given by

$1 \longmapsto s \longmapsto \dfrac{s\pi_L}{\pi_L}$ (s the chosen generator of G).

(6.2.D) *Proposition*

Let L/K be a totally ramified abelian extension of degree p, and let $\xi \in H(\mathcal{O}l_K)$ be a corresponding element. Let t be the largest integer such that $G = G_t$ (where G is the galois group). Then $\vartheta^*(\xi)$ lies in the subgroup $H(U_K/U_K{}^{t+1})$ of $H(U_K)$ and has non zero image in $H(U_K{}^t/U_K{}^{t+1})$.

This is proved by (6.2.B) and (6.2.C) above; cf. also (2.6.D) (iv) and (4.6.D); the element represented by the exact sequence of (6.2.C) is nonzero because $U_L{}^t/U_L{}^{t+1}$ is connected; cf. (6.3.C) for the fact that $H(U_K/U_K{}^{t+1})$ can be considered as a subgroup of $H(U_K)$.

(6.3) **Some lemmas.**

(6.3.A) *Lemma*

Let $0 \to N \to G' \xrightarrow{f} G \to 0$ be an exact sequence of pro-quasi-algebraic groups, and suppose that G,G′ are connected and that $\pi_o(N)(k_s)$ is finite of order h. Then the kernel of f* is finite of order a factor of h.

Proof. The long exact sequence of Hom and Ext groups yields an exact diagram

$$\begin{array}{ccccc}
\mathrm{Hom}(N,(\mathbf{Z}/p\mathbf{Z})_k) & \longrightarrow & \mathrm{Ext}(G,(\mathbf{Z}/p\mathbf{Z})_k) & \longrightarrow & \mathrm{Ext}(G',(\mathbf{Z}/p\mathbf{Z})_k) \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr \\
\mathrm{Hom}(\pi_o(N),(\mathbf{Z}/p\mathbf{Z})_k) & \longrightarrow & H(G) & \xrightarrow{f^*} & H(G')
\end{array}$$

q.e.d.

(6.3.B) The canonical injection $i_n: U_K{}^n/U_K{}^{n+1} \longrightarrow U_K/U_K{}^{n+1}$ defines a homomorphism $i_n^*: H(U_K/U_K{}^{n+1}) \longrightarrow H(U_K{}^n/U_K{}^{n+1})$. Let $e := v_K(p)$; $e_1 := e/(p-1)$.

Lemma (i) If $n < pe_1$ and $p \mid n$, then Im $i_n^* = 0$.
(ii) If $n > pe_1$, then Im $i_n^* = 0$.
(iii) If $n = pe_1$, then $\#(\text{Im } i_n^*) = 1,p$

Proof. Let m be the number $m := n/p$ in case (i) and $m := n-e$ in cases (ii) and (iii). Let $u: U_K \to U_K$ be the morphism $x \longmapsto x^p$. Then u maps $U_K{}^m$ into $U_K{}^n$ and $U_K{}^{m+1}$ into $U_K{}^{n+1}$ and induces epimorphic morphisms $u_m: U_K{}^m/U_K{}^{m+1} \longrightarrow U_K{}^n/U_K{}^{n+1}$ of which the kernel is zero is cases (i) and (ii) and a form of $(\mathbf{Z}/p\mathbf{Z})_k$ in case (iii). Cf. (2.3). Consider the commutative diagram

$$\begin{array}{ccccc} & & U_K^m/U_K^{m+1} & \xrightarrow{u_m} & U_K^n/U_K^{n+1} \\ & \nearrow{\scriptstyle \alpha} & & & \searrow{\scriptstyle i_n} \\ U_K^m/U_K^{n+1} & \xrightarrow{\beta} & U_K/U_K^{n+1} & \xrightarrow{u'} & U_K/U_K^{n+1} \end{array}$$

(α,β the natural morphisms; u' induced by $u(x \longmapsto x^p)$) Applying the functor H yields a commutative diagram

$$\begin{array}{ccccc} & & H(U_K^m/U_K^{m+1}) & \xleftarrow{u_m^*} & H(U_K^n/U_K^{n+1}) \\ & \swarrow{\scriptstyle \alpha^*} & & & \nearrow{\scriptstyle i_n^*} \\ H(U_K^m/U_K^{n+1}) & \xleftarrow{\beta^*} & H(U_K/U_K^{n+1}) & \xleftarrow{(u')^*} & H(U_K/U_K^{n+1}) \end{array}$$

Multiplication with p is zero on $(\mathbf{Z}/p\mathbf{Z})_k$, therefore $(u')^* = 0$, i.e. $\alpha^* u_m^* i_n^* = 0$; α^* is injective because U_K^{m+1}/U_K^{n+1} is connected (cf. lemma (6.3.C) below); therefore $u_m^* i_n^* = 0$. Applying lemma (6.3.A) to u_m we see that Ker $u_m^* = 0$ in cases (i) and (ii) and $\#(\text{Ker } u_m^*) = 1,p$ in case (iii). The same is then true for Im i_n^*, because Im $i_n^* \subset$ Ker u_m^*.

q.e.d.

(6.3.C) *Lemma*

The sequence $0 \to H(U_K^{t'}/U_K^{t}) \to H(U_K^{t'}) \to H(U_K^{t})$ induced by the exact sequence $0 \to U_K^{t} \to U_K^{t'} \to U_K^{t'}/U_K^{t} \to 0$ is exact $(t > t')$.

Proof. This follows from the exact sequence of Hom and Ext groups because U_K^{t} is connected.

q.e.d.

(6.4) **Extensions defined by $X^p - \pi_k$.**

Lemma. If $n = pe_1$, and if there exists an element of $H(U_K/U_K^{n+1})$ with non zero image in $H(U_K^{n}/U_K^{n+1})$, then there exists an element $\xi \in H(\mathcal{O}_K)$ such that $\xi' = \vartheta^*(\xi)$ lies in $H(U_K/U_K^{n+1}) \subset H(U_K)$ and has non zero image in $H(U_K^{n}/U_K^{n+1})$.

Proof in the case that $k = k_s$. The general case will be treated in (6.8). The number e_1 is an integer, therefore there are primitive p-th roots of unity in K (2.2.C). The equation $X^p = \pi_K$ defines a totally ramified abelian extension with galois group isomorphic to $\mathbf{Z}/p\mathbf{Z}$. A generator s of this group maps x onto ζx (where x is some (fixed) root of the equation above and ζ is a primitive p-th root of unity). According to (2.2.B) one has $v_L(\frac{sx}{x} - 1) = v_L(\zeta - 1) = pv_K(\zeta - 1) = pe_1$; therefore $t = pe_1 = n$ (2.5.B). An application of (6.2.D) concludes the proof.

q.e.d.

(6.5) **Artin-Schreier extensions.**

Let n be a positive integer $< pe_1$ and $(n, p) = 1$; let λ be an element of K with $v_K(\lambda) = -n$. Then we have:

(i) The equation $X^p - X = \lambda$ defines a cyclic extension L/K of degree p, which is totally ramified.

(ii) If t is the largest integer such that $G = G_t$ (where $G := G(L/K)$) then $t = n$.

(iii) The element η'_λ of $H(U_K^{n}/U_K^{n+1})$ associated to L/K (cf.(6.2)) is different from zero. And for every $\eta \in H(U_K^{n}/U_K^{n+1})$ there exists a $\lambda \in K$ such that $\eta = \eta'_\lambda$.

Proof. Let x be a root of $X^p - X = \lambda$. Take $L := K(x)$. One of the hypotheses

above is that $v_K(\lambda) < 0$, therefore also $v_L(x) < 0$, and we find that $v_L(x) = p^{-1}v_L(\lambda) = -p^{-1}[L:K]\ n$; but $(n,p) = 1$, therefore $[L:K] = p$; i.e. the equation $X^p - X = \lambda$ is irreducible, and $v_L(x) = -n$.

The equation $(x+Y)^p - (x+Y) - \lambda = Y^p - y - pF(x,Y) = 0$ reduces to $Y^p - Y = 0 \bmod. \pi(K)$. (Because F has integral coefficients; the highest power of x occurring in $F(x,Y)$ is x^{p-1} and $v_L(x^{p-1}) = -(p-1)\ n$, therefore we have that the v_L-value of each coefficient of the polynomial $pF(x,Y)$ in Y is larger than $v_L(p) - (p-1)n = pe - (p-1)n > pe - (p-1)pe_1 = 0$.) The reduced equation $Y^p - Y = 0$ has p different solutions $0,1,\ldots,(p-1)$. By Hensel's lemma there exists p solutions $y_0,\ldots,y_{p-1}$ of $(x+Y)^p - (x+Y) - \lambda = 0$, which have the property $y_i \equiv i \bmod. \pi(L)$. This shows that L/K is galois and cyclic. Choose as a generator the element $s \in G$ which satisfies $sx = x + y_1$.

(ii) Let π_L be a uniformizing element of L. Put $x = \pi_L^{-n}u$, $u \in U(L)$. One has $s\pi_L/\pi_L = 1 + z$, with $v_L(z) = t$ and $su/u \equiv 1 \bmod. (\pi_L^{t+1})$ by the definition of the integer t (cf. (2.5.A.1) and (2.5.B.1)). From this one obtains $\frac{sx}{x} \equiv 1 - nz \bmod. (\pi_L^{t+1})$. On the other hand $sx \equiv x + 1 \bmod (\pi_L)$, therefore also $\frac{sx}{x} \equiv 1 + x^{-1} \bmod. (\pi_L^{n+1})$ Comparing these two expressions for sx/x yields $t = n > 0$ (which shows incidentally that L/K is totally ramified (cf. (2.5.B.1)) and that $-nz \equiv x^{-1} \bmod. (\pi_L^{t+1})$.

(iii) By (6.2.C), η'_λ is represented by the sequence

$$0 \longrightarrow (\mathbf{Z}/p\mathbf{Z})_k \xrightarrow{\gamma} U_L^n/U_L^{n+1} \xrightarrow{N_n} U_K^n/U_K^{n+1} \longrightarrow 0$$

where γ and N_n are as in (6.2.C). Identify $U_L{}^n/U_L{}^{n+1}$ with G_a by means of the morphism $1 - ax^{-1} \longmapsto \bar{a}$ (4.3.5); let f be the composition of γ with this isomorphism; then $f(1) = n^{-1}$; i.e. f is multiplication with n^{-1}. The image of $1 - ax^{-1}$ under N is $N(1 - ax^{-1}) = N(a-x)/N(-x) = (a^p - a - \lambda)/(-\lambda) = 1 - \lambda^{-1}(a^p - a)$. Let $\lambda^{-1} = \pi_K^n\mu$, $\mu \in U(K)$. Let β: $U_K{}^n/U_K{}^{n+1} \to G_a$ be given by $1 + a'\pi_K'' \longmapsto \bar{a}'$ then N_n becomes g: $G_a \to G_a$, $g(a) = -\bar{\mu}(a^p - a)$, $\bar{\mu} \in k^*$. The element of $H(G_a) \simeq k$ (4.6.G) corresponding to

$$0 \to (\mathbf{Z}/p\mathbf{Z})_k \to G_a \to G_a \to 0$$

is $-1/(\bar{\mu}n^{-1}) = -n/\bar{\mu}$ (4.6.G), which is different from zero. Moreover any element $\bar{\nu} \in k^*$ can be obtained in this way by a suitable choice of λ (If ν is any lift of $\bar{\nu}$, take e.g. $\lambda = -\pi_K^n n/\nu$.)

q.e.d.

(6.6) **Proposition.**

The homomorphism $\vartheta^*: H(\mathfrak{o}_K) \to H(U_K)$ is a bijection.

Proof. The homomorphism ϑ is surjective, so ϑ^* is injective. The pro-quasi-algebraic group $\pi(U_K)$ is the projective limit of the pro-quasi-algebraic groups $\pi(U_K/U_K^n)$, therefore $H(U_K)$ is the union of the $H(U_K/U_K^n)$ (6.3.C). We prove by induction that Im ϑ^* contains all the $H(U_K/U_K^n)$. This is true for n = 0. Suppose that Im ϑ^* contains $H(U_K/U_K^n)$, we have the exact sequence (6.3.C)

$$0 \to H(U_K/U_K^n) \to H(U_K/U_K^{n+1}) \to H(U_K^n/U_K^{n+1})$$

It suffices to prove that $H(U_K/U_K^{n+1})$ and $\mathrm{Im}\vartheta^* \cap H(U_K/U_K^{n+1})$ have the same image in $H(U_K^n/U_K^{n+1})$

If $n < pe_1$ and $(n,p) = p$ this is true by (6.3.B) (i).

If $n > pe_1$, this is true by (6.3.B) (ii).

If $n = pe_1$, then Im $H(U_K/U_K^{n+1})$ has at most p elements by (6.3.B) (iii), and if it has more than one element, then Im $(\mathrm{Im}\,\vartheta^* \cap H(U_K/U_K^{n+1})$ has at least p elements by (6.4)

If $n < pe_1$ and $(n,p) = 1$, we have that $\mathrm{Im}(\mathrm{Im}\,\vartheta^* \cap H(U_K/U_K^{n+1}) = H(U_K^n/U_K^{n+1})$ by (6.5).

q.e.d.

(6.7.) **Proof of the theorem.**

Let D_K be the kernel of $\vartheta: \pi(U_K)(k_s) \to \mathfrak{o}_K$. The sequence

$$0 \longrightarrow D_K/D_K \cap p\pi(U_K)(k_s) \longrightarrow \pi(U_K)(k_s)/p\pi(U_K)(k_s) \xrightarrow{\vartheta'} \mathfrak{o}_K/p\,\mathfrak{o}_K \longrightarrow 0$$

is exact. All groups in this sequence are killed by multiplication with p. The dual groups of $\pi(U_K)(k_s)/p\pi(U_K)(k_s)$ and $\mathfrak{o}_K/p\,\mathfrak{o}_K$ are therefore respectively $H(U_K)$ and $H(\mathfrak{o}_K)$. The homomorphism ϑ^* is an isomorphism (6.6), hence so is ϑ'; and we have that $D_K = D_K \cap p\pi(U_K)(k_s)$, i.e. $D_K \subset p\pi(U_K)(k_s)$. By (5.2.C) and the definition of ϑ we known that (cf. especially (5.2.C.1))

$$D_K = \bigcap_{L/K} N_{L/K}\pi(U_L)(k_s),$$

where L runs through all totally ramified abelian extensions of K.

Hence we have, in virtue of (5.2.D) and because $N_{L/K}$ commutes with intersections (AB 5* in $\mathrm{Pro}(CQG_k)$; cf. (4.1))

$$N_{L/K}(D_L) = N_{L/K}(\bigcap_{M/L} N_{M/L}\pi(U_M)(k_s) = \bigcap_{M/K} N_{M/K}\pi(U_M)(k_s) \supset D_K$$

where M runs through all abelian totally ramified extensions of L. Hence

$$D_K \subset \bigcap_{L/K} N_{L/K}(D_L) \subset \bigcap_{L/K} p\, N_{L/K}(\pi(U_L)(k_s) \subset p \bigcap_{L/K} N_{L/K}\pi(U_L)(k_s) = pD_K$$

D_K is a pro-p-group (= projective limit of finite p-groups) (6.1) and $D_K \subset pD_K$, this shows that $D_K = 0$.

q.e.d.

We have now proved the theorem in the case that $k = k_s$, and when k is not necessarily algebraically closed we have proved the theorem up to lemma (6.4)

(6.8) **Proof of lemma (6.4).**

Let

$$(*) \qquad 0 \longrightarrow (\mathbf{Z}/p\mathbf{Z})_k \longrightarrow Y \xrightarrow{f} U_K/U_K^{n+1} \longrightarrow 0$$

represent an element of $H(U_K/U_K^{n+1})$ which is not in $H(U_K/U_K^{n})$, then Y is connected, hence absolutely connected. We now that $\mathrm{Im}(H(U_K/U_K^{n+1}) \subset H(U_K^{n}/U_K^{n+1}$ has exactly p elements. For by the hypothesis of (6.4) there are at least p elements in $\mathrm{Im}(H(U_K/U_K^{n+1})$ and at most there are p according to (6.3.B). We also know that there are exactly p elements in $\mathrm{Im}\, H((U_K/U_K^{n+1})_{k_s})$ and that a generator of this subgroup of p elements is any of the elements associated with the extension $\hat{K}_{nr}(x)/\hat{K}_{nr}$ where x is a root of the polynomial $X^p - \pi_K$. By the theorem in the algebraically closed case therefore there must be an isomorphism φ

$$\begin{array}{ccccccc} 0 \to (\mathbf{Z}/p\mathbf{Z})_{k_s} & \to & U^n_{\hat{L}_{nr}}/U^{n+1}_{\hat{L}_{nr}} & \to & U^n_{\hat{K}_{nr}}/U^{n+1}_{\hat{K}_{nr}} & \to 0 \\ \downarrow & & \downarrow \varphi & & \downarrow \wr & \\ 0 \to (\mathbf{Z}/p\mathbf{Z})_{k_s} & \to & Y'_{k_s} & \to & (U_K^n/U_K^{n+1})_{k_s} & \to 0 \end{array}$$

between the upper exact sequence, where $\hat{L}_{nr} := \hat{K}_{nr}(x)$, and the lower exact sequence, which represents the image of (*) in $H((U_K^n/U_K^{n+1})_{k_s})$ (after base change $k \longrightarrow k_s$). Lemma (4.7) shows that φ commutes with the action of $G(k_s/k)$. The images of $\mathbf{Z}/p\mathbf{Z}$ in $U^n(\hat{L}_{nr})/U^{n+1}(\hat{L}_{nr})$ come from the p-th roots

of unity, which are contained in $\hat{K}_{nr}$ because e_1 is an integer (2.2.C). Therefore the p-th roots of unity in $U(\hat{K}_{nr})$ are invariant mod. $U^{e_1+1}(\hat{K}_{nr})$ under the action of $G(k_s/k) \simeq G(K_{nr}/K)$ (as (*) has a constant kernel); i.e. they can be written in the form $1 + \pi_K^{e_1} a + \pi_K^{e_1+1} b$ with $a \in A(K)$. In fact we can certainly write the p-th roots of unity in $U(\hat{K}_{nr})$ as $1 + \pi_K^{e_1} a' + \pi_K^{e_1+1} b'$ with $a', b' \in A(\hat{K}_{nr})$. Let $\bar{a}'$ be the image of a' in k_s, from the fact that the p-th roots of unity are invariant mod. $U^{e_1+1}(\hat{K}_{nr})$ we see that $s(\bar{a}') = \bar{a}'$ for all $s \in G(k_s/k)$ hence that $\bar{a}' \in k$; let a be lift of $\bar{a}'$, $a \in A(K)$, then $a' = a + \pi_K y$. The polynomial

$$\pi_K^{-pe_1}(1 + \pi_K^{e_1} X)^p - 1$$

is monic, has all its coefficients in A(K), and has what was shown above p different roots mod.(π_K). Hence by Hensel's lemma there are roots in A(K). We have proved that the p-th roots of unity are in K. The extension K(x)/K where x is any root of $X^p - \pi_K$ defines the desired element of $H(\mathfrak{A}_K)$. In fact the largest integer t such that $G_t = G$ (where $G := G(K(x)/K)$) is equal to $pe_1 = n$ ((2.2.B) and (2.5.B.1)). It now suffices to apply (6.2.D) (exactly as in the last few lines of (6.4)).

q.e.d.

7. SECOND PROOF OF THE THEOREM. RAMIFICATION.

Assume that theorem (5.4.D) is proved when $k = k_s$ (cf. § 6 or [CAC]). From this it is possible, by means of the same kind of considerations as those we earlier met with in (6.8) ('descent'), to deduce a second proof of theorem (5.4.D). In (7.4) we describe the ramification subgroups of $\mathfrak{A}_K$.

(7.1) Action of $G(k_s/k)$.

Let L/K be a finite galois extension of K. ((2.1) shows that for every finite abelian extension E of $\hat{K}_{nr}$ there exists a finite galois L/K such that $E \subset \hat{L}_{nr}$). The pro-quasi-algebraic groups U_L and V_L are not a priori defined over k but only over the residue field l of L. However there still exists a natural action of $G(k_s/k)$ on $U_L/V_L(k_s) \simeq U(\hat{L}_{nr})/V(\hat{L}_{nr})$. Let $s \in G(k_s/k)$ and $s' \in G(L_{nr}/K)$ any lift of s. Define $s(\bar{u}) := \overline{s'(u)}$, where u represents $\bar{u} \in U(\hat{L}_{nr})/V(\hat{L}_{nr})$. (As usual, $v \mapsto \bar{v}$ is the canonical homomorphism onto a quotient). This definition does not depend on the choice of s'; for let ts' be any other lift of s (where $t \in G(L/K)_{ram}$) then $ts'(u) = \frac{ts'(u)}{s'(u)} \cdot s'(u) \equiv s'(u) \bmod. V(\hat{L}_{nr})$.

Remark.

This action of $G(k_s/k)$ is analogous to the second action of $G(k_s/k)$ on $U_K(k_s)$ defined in section (5.1.A). In fact it is not difficult to 'descend' U_L/V_L. Let L'/K be finite totally ramified extension such that $L'.K_{nr} = L.K_{nr}$ (2.8.E). Let $V_{L'}$ be the connected component of the identity of the kernel of the norm morphism $N_{L'/K} : U_{L'} \to U_K$. Then $(U_{L'}/V_{L'})_l \simeq U_L/V_L$ (4.7) and the action of $G(k_s/k)$ on $U_L/V_L(k_s) \simeq U_{L'}/V_{L'}(k_s)$ as described above is identical with the natural action induced by the k-pro-quasi-algebraic structure of $U_{L'}/V_{L'}$. (5.1.A).

(7.2) **Lemma**

Let L/K be a finite galois extension. The homomorphism $N: U(\hat{L}_{nr})/V(\hat{L}_{nr}) \to U(\hat{K}_{nr})$ commutes with the action of $G(k_s/k)$.

Proof. Let $s \in G(k_s/k)$ and let $s' \in G(L_{nr}/K)$, $s'' \in G(K_{nr}/K)$ be lifts of s then $s'|\hat{K}_{nr} = s''$. Let $G(L/K)_{ram} = \{t_1, \ldots, t_e\}$, $u \in U(\hat{L}_{nr})$, then $s''(t_1 u. \ldots .t_e u) = s'(t_1 u. \ldots .t_e u) = t_1 s'u. \ldots .t_e s'u$ for $G(L/K)_{ram} = G(\hat{L}_{nr}/\hat{K}_{nr})$ is normal in $G(L_{nr}/K)$.

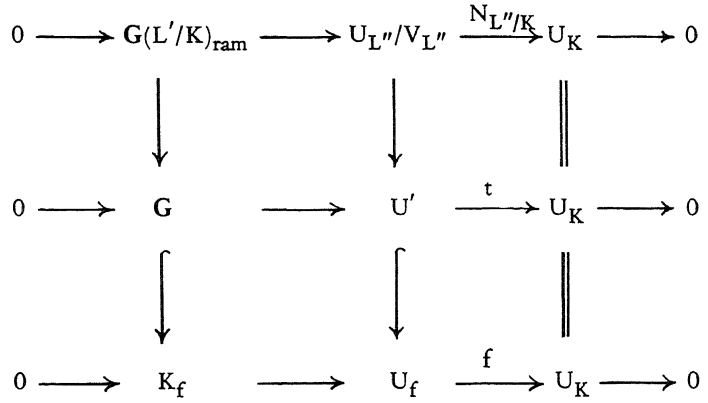
q.e.d.

(7.3) **Proof of the theorem.**

According to (5.4.C) (surjectivity of ϑ) we only have to prove that there are sufficiently many totally ramified abelian extensions; we have to prove that if

$$0 \longrightarrow K_f \longrightarrow U_f \xrightarrow{f} U_K \longrightarrow 0$$

is an isogeny with constant kernel, then there exists a totally ramified abelian extension M/K such that the norm morphism $N_{M/K}: U_M/V_M \to U_K$ factors through f. We now, from the theorem when $k = k_s$, that there exists an abelian extension $P/\hat{K}_{nr}$ such that $U_P/V_P \to U_{\hat{K}_{nr}}$ factors through $f \otimes_k k_s$. Enlarging P if necessary we can assume by (2.1.D) that P is of the form $P = L'_{nr}$ for a certain finite galois extension L'/K (which has the property that $G(L'/K)_{ram}$ is abelian). Let L''/K be a totally ramified extension such that $L''.K_{nr} = L'.K_{nr}$ (2.8.E); $V_{L''}$ the connected component of the identity of the kernel of $N_{L''/K}: U_{L''} \to U_K$. We have that $(U_{L''}/V_{L''})_{k_s} \simeq (U_{L'}/V_{L'})_{k_s}$ and that $U_{L''}/V_{L''} \to U_K$ factors through f ((4.7), cf. also (5.4.B)). Let U' be the image of $U_{L''}/V_{L''}$ in U_f. We have a commutative diagram



$K_f(k_s)$ is left pointwise fixed under the action of $G(k_s/k)$, hence the kernel H of the induced homomorphism $G(L'/K)_{ram} \simeq \mathbf{G}(L'/K)_{ram}(k_s) \to \mathbf{G}(k_s)$ is stable under this action (which is the action by inner automorphisms (5.1.B)). This proves that H is a normal subgroup not only of $G(L'/K)_{ram}$ but also of $G(L'/K)$ itself. Let L be the invariant field of H. Then $(U')_{k_s} \simeq (U_L/V_L)_{k_s}$ and t becomes the norm map under this isomorphism. One can descend U_L/V_L, cf. Remark (7.1), accordingly the injection $U_L/V_L(k_s) \hookrightarrow U_f(k_s)$ commutes with the action of $G(k_s/k)$ (or apply (4.7) once more). This shows that $G(L/K)_{ram} \subset G(k_s)$ is left pointwise fixed under the action of $G(k_s/k)$. i.e. that $G(L/K)_{ram} \subset Z(G(L/K))$. By the pullback theorem (2.8.G) there exists an abelian totally ramified extension M/K such that $M_{nr} = L_{nr}$. By (5.4.B) we have $(E_{L/K})_{k_s} = (E_{M/K})_{k_s} = E_{k_s}$ if E denotes the element represented by the middle extension in the diagram above. Hence (4.7) $E_{M/K} = E$ and we are through.

q.e.d.

(7.4) **Ramification.**

(7.4.A) THE ψ-FUNCTION AND HERBRAND'S THEOREM.

Let L/K be a finite galois extension with galois group G and ramification subgroups G_i ($s \in G_i \Leftrightarrow (v_L(sa - a) \geqslant i+1$ for all $a \in A(L)$)). It is clear that

(7.4.A.1) $G(L/M)_i = G(L/M) \cap G(L/K)^i$ if M is a sub-extension of L.

We define $\varphi_{L/K}(x) = x \qquad -1 \leqslant x \leqslant 0$

$\varphi_{L/K}(x) = \frac{1}{g_0}(g_1 + \ldots + g_m + (x-m)g_{m+1}) \qquad m \leqslant x \leqslant m+1,\ m+1 \in \mathbf{N}$

where $g_i := \#G_i$. The function $\varphi_{L/K} : [-1,\infty) \to [-1,\infty)$ is monotonically in-

creasing. Let $\psi_{L/K}$ be the inverse function of $\varphi_{L/K}$. Note that this function coincides with the one defined in (2.6) when L/K is totally ramified galois of prime degree.

(7.4.A.2) *Lemma*

If $L \supset M$ are both galois extensions of K, then

$$\psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}.$$

For a proof cf. [CL] Ch.IV § 3 Prop. 15.

We now define ramification groups with upper indices G^i by means of the formula

$$G^i := G_{\psi(i)}$$

Note that $\psi(i)$ is an integer if i is an integer.
These ramification groups behave nicely with respect to quotients in the sense of:

(7.4.A.3) *(Herbrand's theorem)*

If M/K and L/K are both galois extensions and $M \subset L$, then the natural projection $G(L/K) \to G(M/K)$ maps $G(L/K)^i$ onto $G(M/K)^i$.

For a proof cf. [CL] Ch.IV § 3 Prop. 14 and Lemma 5.

Herbrand's theorem makes it possible to define $G(L/K)^i$ also for infinite galois extensions L/K by means of the formula

$$G(L/K)^i := \varprojlim G(M/K)^i,$$

where M runs through all finite galois sub-extensions of L. In particular we can define $\mathfrak{o}_K^i$ for $i \geqslant 0$

$$\mathfrak{o}_K^i := G(K^{ab}/K)^i.$$

Remark that $\psi_{K_n/K}(x) = x$ if K_n/K is unramified; it follows that ((7.4.A.1) and (7.4.A.2)):

$$G(L/K)^i = G(L/K_L)^i, \qquad i \geqslant 0,$$

where K_L is the maximal unramified extension of K contained in L.

(7.4.B) SOME EXACT SEQUENCES.

Let L/K be a totally ramified abelian extension. Then we have a sequence

(7.4.B.1) $0 \longrightarrow (G(L/K)^n)_k \xrightarrow{i^n} U_L^{\psi(n)}/V_L \cap U_L^{\psi(n)} \xrightarrow{N^n_{L/K}} U_K^n \longrightarrow 0$

It is clear that i^n is monomorphic, and that $N^n_{L/K}$ is epimorphic ((5.2.B.1), (2.6.D) and (7.4.A.2)).

(7.4.B.2) *Lemma*

The sequence (7.4.B.1) is exact if L/K is of prime degree.

Proof. Let t be the largest integer such that $G_t = G$ (where $G = G(L/K)$). For $n \leqslant t$, the exactness of (7.4.B.1) follows from (5.2.B.1) (cf. also (2.7.A.3) and (2.5.B.1)). If $n > t$, then $G^n = G_{\psi(n)} = \{1\}$. Let $x \in U_L^{\psi(n)}(k_s)$ be such that $N^n_{L/K}(x) = 1$. Then $x \in \frac{s\pi_L}{\pi_L} V_L(k_s)$ for a certain $s \in G$ (5.2.B.1). Suppose $s \neq 1$, then $\frac{s\pi_L}{\pi_L} \in U_L^t(k_s) \setminus U_L^{t+1}(k_s)$, and hence also $\frac{s\pi_L}{\pi_L} \cdot V_L(k_s) \subset U_L^t(k_s) \setminus U_L^{t+1}(k_s)$ because $V_L(k_s) \subset U_L^{t+1}(k_s)$ (cf. (2.5.A.1)). Therefore, as $n > t$, $\frac{s\pi_L}{\pi_L} V_L(k_s) \cap U_L^{\psi(n)}(k_s) = \phi$ if $s \neq 1$. This shows that $x \in V_L(k_s)$.

q.e.d.

(7.4.B.3) *Lemma*

$U_L^{\psi(n)} \cap V_L$ is the connected component of the identity of the kernel of $N^n_{L/K}$ if L/K is of prime degree. (n=0, 1, ...).

Proof. It is clear that $U_L^{\psi(n)} \cap V_L$ contains $(\mathrm{Ker}(N^n_{L/K}))^\circ$ because the quotient $(\mathrm{Ker}\, N^n_{L/K})/U_L^{\psi(n)} \cap V_L$ is a subgroup of $(G(L/K))_k$ and hence finite (5.2.B.1). (This holds also for not necessarily cyclic L/K). If $n \leqslant t$, then $\psi(n) = n$ and $U_L^n \cap V_L = U_L^n \cap U_L^{t+1} \cap \mathrm{Ker}\, N_{L/K} = U_L^{t+1} \cap \mathrm{Ker}\, N_{L/K} = V_L$ is connected (2.7.B.1). Let $n > t$. It is clear that the kernel of the induced morphism $U_L^{\psi(n)}/U_L^{\psi(n+1)} \xrightarrow{\overline{N}^n_{L/K}} U_K^n/U_K^{n+1}$ is $\mathrm{Ker}\, N^n_{L/K}/\mathrm{Ker}\, N^{n+1}_{L/K}$. As $\overline{N}^n_{L/K}$ is zero on $U_L^{\psi(n)+1}/U_L^{\psi(n+1)}$ and the induced morphism $U_L^{\psi(n)}/U_L^{\psi(n)+1} \longrightarrow U_K^n/U_K^{n+1}$ is an isomorphism (2.6.D) (v), it follows that $\mathrm{Ker}\, N^n_{L/K}/\mathrm{Ker}\, N^{n+1}_{L/K} \simeq U_L^{\psi(n)+1}/U_L^{\psi(n+1)}$ is connected. Therefore $\mathrm{Ker}\, N^n_{L/K}$ itself is also connected

(being the projective limit of the $\mathrm{Ker}\, N^{n}_{L/K}/\mathrm{Ker}\, N^{n+m}_{L/K}$).

q.e.d.

(7.4.B.4) *Proposition*

a) The sequence (7.4.B.1) is exact for all totally ramified abelian extensions L/K.

b) $U_L^{\psi_{L/K}(n)} \cap V_{L/K}$ is the connected component of the identity of the kernel of $N^{n}_{L/K}\colon U_L^{\psi_{L/K}(n)} \to U_K^n$.

(We here write $V_{P/P'}$ for the connected component of the identity of the morphism of pro-quasi-algebraic groups $N_{P/P'}\colon U_P \to U_{P'}$; i.e. $V_{L/K} = V_L$).
Proof. We prove a) and b) simultaneously by induction on [L: K]. Lemmas (7.4.B.2) and (7.4.B.3) prove the proposition when L/K is of prime degree. If L/K is not of prime degree, let M be a sub-extension of L. We have a commutative diagram

(7.4.B.5)

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & (G(L/M)_{\psi_{L/K}(n)})_k & = & (G(L/M)_{\psi_{L/K}(n)})_k & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & (G(L/K)_{\psi_{L/K}(n)})_k & \longrightarrow & U_L^{\psi_{L/K}(n)}/V_{L/K} \cap U_L^{\psi_{L/K}(n)} & \xrightarrow{N^n_{L/K}} & U_K^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow N_{L/M}^{\psi_{M/K}(n)} & & \| & & \\
0 & \longrightarrow & (G(M/K)_{\psi_{M/K}(n)})_k & \longrightarrow & U_M^{\psi_{M/K}(n)}/V_{M/K} \cap U_M^{\psi_{M/K}(n)} & \xrightarrow{N^n_{M/K}} & U_K^n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

The first column is exact according to (7.4.A.1) – (7.4.A.3). By the induction hypothesis we know that the third row of the diagram is exact and that the sequence

$$0 \to (G(L/M)_{\psi_{L/K^{(n)}}})_k \to U_L^{\psi_{L/K^{(n)}}}/U_L^{\psi_{L/K^{(n)}}} \cap V_{L/M} \to U_M^{\psi_{M/K^{(n)}}} \to 0$$

is exact. Hence $N_{L/M}^{\psi_{M/K^{(n)}}}$ induces an epimorphism $\operatorname{Ker} N_{L/K}^n \to \operatorname{Ker} N_{M/K}^n$ and an epimorphism $V_{L/K} \cap U_L^{\psi_{L/K^{(n)}}} \to V_{M/K} \cap U_M^{\psi_{M/K^{(n)}}}$ because $V_{L/K} \cap U_L^{\psi_{L/K^{(n)}}}$ contains the connected component of the identity of $\operatorname{Ker} N_{L/K}^n$ and is mapped into $V_{M/K} \cap U_M^{\psi_{M/K^{(n)}}}$, which is the connected component of the identity of $\operatorname{Ker} N_{M/K}^n$ by the induction hypothesis. An application of the snake lemma ([2] §1 Prop. 2) yields that the third row in the diagram below (which is the second column in the diagram (7.4.B.5)) is exact.

$$\begin{array}{ccccc}
 & & V_{L/K} \cap U_L^{\psi_{L/K^{(n)}}}/V_{L/M} \cap U_L^{\psi_{L/K^{(n)}}} & \xrightarrow{\alpha} & V_{M/K} \cap U_M^{\psi_{M/K^{(n)}}} \\
 & & \downarrow & & \downarrow \\
0 \to (G(L/M)_{\psi_{L/K^{(n)}}})_k & \to & U_L^{\psi_{L/K^{(n)}}}/V_{L/M} \cap U_L^{\psi_{L/K^{(n)}}} & \to & U_M^{\psi_{M/K^{(n)}}} \to 0 \\
\| & & \downarrow & & \downarrow \\
0 \to (G(L/M)_{\psi_{L/K^{(n)}}})_k & \to & U_L^{\psi_{L/K^{(n)}}}/V_{L/K} \cap U_L^{\psi_{L/K^{(n)}}} & \to & U_M^{\psi_{M/K^{(n)}}}/V_{M/K} \cap U_M^{\psi_{M/K^{(n)}}} \to 0
\end{array}$$

It then follows that α is an isomorphism. This implies that $V_{L/K} \cap U_L^{\psi_{L/K^{(n)}}}$ is connected because both $V_{L/M} \cap U_L^{\psi_{L/K^{(n)}}}$ and $V_{M/K} \cap U_M^{\psi_{M/K^{(n)}}}$ are connected by the induction hypothesis. This takes care of b). An application of the snake lemma in diagram (7.4.B.5) (in which the second column is now also exact) proves that the second row is exact.

q.e.d.

(7.4.C) THE RAMIFICATION GROUPS OF $\mathcal{O}_K$.

The diagram

$$\begin{array}{ccccccc} 0 \to (G(L/K))_k & \to & U_L^{\psi(n)}.\mathrm{Ker}\, N_{L/K}/V_L & \to & U_K^n & \to 0 \\ \| & & \downarrow & & \downarrow & \\ 0 \to (G(L/K))_k & \to & U_L/V_L & \to & U_K & \to 0 \end{array}$$

has a cartesian righthand square because $U_L^{\psi(n)} \to U_K^n$ is epimorphic. (We write $\psi(n)$ for $\psi_{L/K}(n)$). The pro-quasi-algebraic group $U_L^{\psi(n)}$. $\mathrm{Ker}\, N_{L/K}/V_L$ is not necessarily connected. Its connected component of the identity is $U_L^{\psi(n)}.V_L/V_L \simeq U_L^{\psi(n)}/V_L \cap U_L^{\psi(n)}$. We have an exact diagram (7.4.B.4)

$$\begin{array}{ccccccc} 0 \to (G(L/K)^n)_k & \to & U_L^{\psi(n)}/V_L \cap U_L^{\psi(n)} & \to & U_K^n & \to 0 \\ \downarrow & & \downarrow & & \downarrow & \\ 0 \to (G(L/K))_k & \to & U_L/V_L & \to & U_K & \to 0 \end{array}$$

As $U_L^{\psi(n)}/V_L \cap U_L^{\psi(n)}$ is connected, it follows that $(G(L/K)^n)_k$ is a quotient of $\mathfrak{p}(U_K^n)$. We have found the theorem:

(7.4.C.1) *Theorem*

The image of $\mathfrak{p}(U_K^n)(k_s)$ in $\mathfrak{p}(U_K)(k_s)$ corresponds to $\mathcal{O}_K^n$ under the isomorphism $\mathfrak{p}(U_K)(k_s) \simeq \mathcal{O}_K$.

We know that $\pi_1(U_K^n)(k_s) \to \pi_1(U_K)(k_s)$ is injective because π_1 is left exact. Therefore

(7.4.C.2) *Corollary* ([CAC] Th.1).

When $k = k_s$, then $\vartheta: \pi_1(U_K)(k_s) \simeq \mathcal{O}_K$ induces an isomorphism $\pi_1(U_K^n)(k_s) \simeq \mathcal{O}_K^n$.

8. INFINITESIMAL CONSIDERATIONS.

Let L/K be a totally ramified galois extension. In this section we study the infinitesimal part of the kernel of the morphism $N_{L/K}$ between the pro-algebraic group schemes U_L and U_K. We work in the category $Pro(CG_k)$. The pro-algebraic group schemes U_L and U_K are reduced (4.3.6). In characteristic zero all algebraic group schemes are reduced (Theorem of Cartier, see e.g. [14]), hence we shall assume in this section that the characteristic of the residue field k is different from zero. It turns out that a totally ramified galois extension L/K is tamely ramified iff Ker $N_{L/K}$ is reduced.
The propositions (8.3.C) and (8.5.C) are stated for all totally ramified galois extension L/K and proved only for cyclic L/K of prime order. One deduces the propositions for not necessarily prime order, totally ramified, galois L/K from this by considering towers $K = K_0 \subset K_1 \subset \ldots \subset K_m = L$ of cyclic extensions. (One can find such a tower for each L/K because G(L/K) is solvable (2.5.B.4)). For (8.3.C) (ii) and (8.5.C) this procedure yields the propositions immediately; for (8.3.C) (i) one needs in addition (cf. (7.4.A))

1° a ψ-function defined for all galois L/K

2° the transitivity of these functions. (I.e. $\psi_{M/K} \cdot \psi_{L/K}$ when $K \subset L \subset M$).

Acknowledgements must be made to Prof. P. Gabriel for this section.

If U is an algebraic group scheme, Lie U denotes the tangent Lie-algebra of U. By definition Lie U := Ker $(U(k[\epsilon]) \to U(k))$, where $k[\epsilon]$ is short for $k[X]/(X^2)$; i.e. $\epsilon^2 = 0$.

As to the contents of this section: we first list some facts about the trace and norm maps in (8.1). Then we show in (8.2) that the kernel of the norm morphism $U_L \to U_K$ is not reduced for wildly ramified extensions. After having devoted some space to what $W_n(k[\epsilon])$ looks like in (8.4) we then look more closely at the equal characteristic case (char(K) = p) in (8.3), and at the unequal characteristic case (char(K) = 0) in (8.5).

(8.1) Some facts about trace and norm.

Let L/K be a totally ramified galois extension of prime degree l; let t be the largest integer such that $G = G_t$ (cf.(2.5)) Then

$$(8.1.1) \qquad Tr(\pi_L^n A(L)) = \pi_K^r A(K), \qquad r = \left[\frac{(t+1)(l-1)+n}{l}\right].$$

If L/K is tamely ramified ($\Leftrightarrow (t = 0) \Leftrightarrow ((l,p) = 1)$), then Tr | A(K) is multiplication by l, so we have

(8.1.2) $\quad Tr(A(L)) = Tr(A(K)) = A(K)$ $\quad$ if L/K is tamely ramified.

From (2.6.E) follows that

(8.1.3) $\quad N(U_L^{\psi(n)}) = U_K^n, \qquad N(U_L^{\psi(n)+1}) = U_K^{n+1}$

where ψ is the function $\psi(x) = x$ if $x \leqslant t$, $\psi(x) = t + l(x-t)$ if $x \geqslant t$. From this it is not difficult to see that for sufficiently large n

(8.1.4) $\quad N(U_L^{nle}) = U_K^z \qquad$ where $z = [ne + t + 1 - \frac{t+1}{l}]$.

If $\psi(r-1) + 1 \leqslant s \leqslant \psi(r)$ we have by (8.1.1)

(8.1.5) $\quad Tr(\pi_L^s A(L)) = \pi_K^r A(K) \qquad$ if $r-1 \geqslant t$.

Combining (8.1.3) and (8.1.5) we obtain that

(8.1.6) $\quad Tr(\pi_L^s A(L)) = \pi_K^r A(K) \Leftrightarrow N(U_L^s) = U_K^r \qquad$ for large enough r,s.

(8.2) **Wildly ramified extensions.**

Let L/K be a wildly and totally ramified galois extension. Its degree [L:K] is then divisible by p. We have $U_L \simeq G_m \times U_L^1$, $U_K \simeq G_m \times U_K^1$. The norm morphism maps the factor G_m into the factor G_m. One easily sees that the induced morphism is multiplication with [L : K]; i.e. $x \mapsto x^n$ when n = [L : K]. The kernel of this morphism is not reduced. We have found that

(8.2.1) $\quad X_{inf} := X/X_{red} \neq 0, \qquad$ for wildly and totally ramified galois L/K,

where X denotes the kernel of $N: U_L \to U_K$.

(8.3) **The equal characteristic case.**

In this section we assume that char(k) = char(K) = $p \neq 0$.

(8.3.A) *Lemma*

$$\text{Lie } U_L/U_L^s \simeq A(L)/\pi_L^s A(L) \qquad \text{(as a vector space)}$$
$$\text{Lie } N_{L/K} \simeq Tr_{L/K}: A(L) \to A(K).$$

Proof. Lie $U_L/U_L^s := \mathrm{Ker}(U_L/U_L^s(k[\epsilon]) \to U_L/U_L^s(k))$
$= \mathrm{Ker}\,(\mathrm{units}((A(L)/\pi_L{}^sA(L) \otimes_k k[\epsilon]) \to \mathrm{units}\,(A(L)/\pi_L{}^sA(L))$
$= (A(L)/\pi_L{}^sA(L))$. (Cf. (4.2.7)).
$N_{L/K}(1 + \epsilon a) = (1 + \epsilon s_1(a)) \ldots (1 + \epsilon s_1(a)) = 1 + \mathrm{Tr}(a)\,\epsilon$.

q.e.d.

Let $\mathrm{Tr}(A(L)) = \pi_K^{r_0}A(K)$, then $r_o \geqslant 0$ and $(r_o > 0) \Leftrightarrow$ (L/K is wildly ramified).
Let s and $r > r_o$ be such that $N_{L/K}(U_L{}^s) = U_K{}^r$; let $X^s := \mathrm{Ker}(U_L/U_L{}^s \to U_K/U_K{}^r)$
Then we have:

(8.3.B) *Lemma*

$$\dim(\mathrm{Lie}\,(X^s)_{inf}) = r_o.$$

Proof. The sequence $o \to X^s \to U_L/U_L{}^s \to U_K/U_K{}^r \to 0$ is exact, from which we obtain an exact sequence

$$0 \to \mathrm{Lie}\,X^s \to A(L)/\pi_L^sA(L) \to A(K)/\pi_K^rA(K)$$

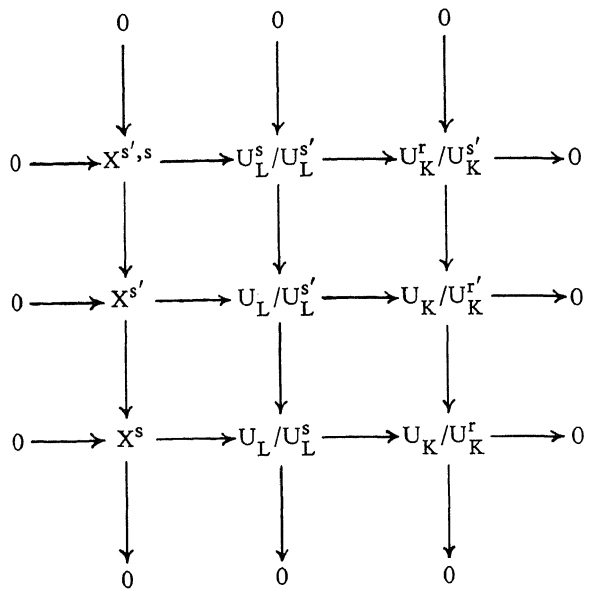
(8.3.A); dim X^s = s–r; dim Lie X^s = $\dim(A(L)/\pi_L^sA(L)) - \dim\,(\mathrm{Im}(A(L)/\pi_L^sA(L)))$ =
$= s - (r - r_o) = s - r + r_o$. Hence $\dim(\mathrm{Lie}\,(X^s)_{inf}) = r_o$.

q.e.d.

(8.3.C) *Proposition*

Let L/K be a totally ramified galois extension; let $X := \mathrm{Ker}\,(U_L \longrightarrow U_K)$.
Then we have
(i) dim (Lie X_{inf}) = r_o is finite (r_o as above)
(ii) $(X_{inf} = o) \Leftrightarrow$ (L/K is tamely ramified).

Proof. (ii) follows from (i), for r_o is determined by $\mathrm{Tr}(A(L)) = \pi_K^{r_o}A(K)$ and $\mathrm{Tr}(A(L)) = A(K)$ iff L/K is tamely ramified. Let (s', r') and (s, r) be two pairs such that $N(U_L{}^{s'}) = U_K{}^{r'}$, $N(U_L{}^s) = U_K{}^r$, $s' > s$ and $r' > r$.
We have an exact diagram



Tr: $\pi_L^s A(L)/\pi_L^{s'} A(L) \to \pi_K^r A(K)/\pi_K^{r'} A(K)$ is surjective for large enough r (8.1.6). Therefore $\dim(\mathrm{Lie}(X^{s',s})_{inf}) = 0$ if s',s are large enough. Using (8.3.B) and dimension counting we obtain $X_{inf} = (X^s)_{inf}$ for large s and hence (i).

q.e.d.

(8.4) $W_n(k[\epsilon])$.

To find the dimension of Lie X_{inf} in the unequal characteristic case, we need to know what $W_n(k[\epsilon])$ looks like.
The addition and multiplication on $W_n(A)$ (for any commutative ring A) are given by polynomials $S_0,S_1,\ldots,S_{n-1}; P_0,\ldots,P_{n-1} \in \mathbf{Z}[X_0,\ldots,X_{n-1}; Y_0,\ldots,Y_{n-1}]$ which satisfy

$$W_i(S_0,\ldots,S_i) = W_i(X) + W_i(Y),$$
$$W_i(P_0,\ldots,P_i) = W_i(X).W_i(Y),$$

where $W_0(X) := X_0; W_1(X) = X_0^p + pX_1; \ldots; W_i(X) := X_0^{p^i} + pX_1^{p^{i-1}} + \ldots + p^iX_i$.
Recursively this gives for the S_i and P_i

$$(8.4.1) \qquad S_0 = X_0+Y_0 \qquad S_i = \frac{W_i(X) + W_i(Y) - W_{i-1}(S_0^p,\ldots,S_{i-1}^p)}{p^i},$$

(8.4.2) $P_o = X_o.Y_o \qquad P_i = \dfrac{W_i(X).W_i(Y) - W_{i-1}(P_o^p,\ldots,P_{i-1}^p)}{p^i}$.

Let ϵ_j (j = 0,...,n−1) be the element (0,...,0, ϵ, 0,...,0) of $W_n(k[\epsilon])$ (ϵ on the j−th place). Using (8.4.2) one easily finds that in $W_n(k[\epsilon])$

(8.4.3) $\epsilon_j(a_o,\ldots,a_{n-1}) = (0,0,\ldots,0,W_j(a_o,\ldots,a_j)\,\epsilon,0,\ldots,0)$,

where $(a_o,\ldots,a_{n-1}) \in W_n(k)$ for any ring k. And thus especially

(8.4.4) $\epsilon_j(a_o,..,a_{n-1}) = (0,\ldots,0,a_o^{p^j}\epsilon,0,..,0)$ when char(k) = p.

In the same way one finds that

(8.4.5) $\epsilon_i\epsilon_j = 0$ for all i,j = 0,1,..,n−1.

From (8.4.4) and (8.4.5) one now sees that, when char(k) = p

(8.4.6) $W_n(k[\epsilon]) = W_n(k) + \sum_{i=0}^{n-1} k\,\epsilon_i$, the sum being direct.

(8.5) **The unequal characteristic case.**

We assume in this section that char(K) = 0, char(k) = p ≠ 0. Let e be the absolute index of ramification of K (i.e. $e = e_K = v_K(p)$) $e_L = [L : K]e$ when L/K is totally ramified of degree l. The module $A(K)/\pi_K^{ne}A(K)$ is free of rank n over $W_n(k)$.

(8.5.A) *Lemma*

$$\text{Lie}\,(U_L/U_L^{nel}) \simeq \sum_{i=0}^{n-1} (A(L)/pA(L))\,\epsilon_i$$

Proof. Lie $(U_L/U_L^{nel}) := \text{Ker}(\text{Units}((A(L)/\pi_L^{nel}A(L)) \otimes_{W_n(k)} W_n(k[\epsilon])) \to$ Units $(A(L)/\pi_L^{nel}A(L))) = \sum_{i=0}^{n-1} (A(L)/pA(L))\,\epsilon_i$ (cf.(4.2.7), (8.4.6)).

q.e.d.

(8.5.B) *Lemma*

Let n,n' be such that $N(U_L^{nel}) = U_K^{n'e}$. The induced map Lie N: Lie $U_L/U_L^{nel} \to$ Lie $U_K/U_K^{n'e}$ is then the trace map on each of the summands $(A(L)/pA(L))\epsilon_i$.

(8.5.C) *Proposition*

(L/K tamely ramified) $\Leftrightarrow X_{inf} = 0$ (where again $X := \mathrm{Ker}\,(U_L \longrightarrow U_K)$).

Proof. From (8.1.4) we see (t=0) that $N(U_L^{ne}) = U_K^{ne}$, when L/K is tamely ramified. We have an exact sequence

$$0 \to X^n \to U_L/U_L^{nel} \to U_K/U_K^{ne} \to 0$$

On A(K)/pA(K), the trace map is given by multiplication with l, which is prime to p; hence Tr: $A(L)/pA(L) \to A(K)/pA(K)$ is surjective, and we find $(X^n)_{inf} = 0$ for all n. The opposite implication is proved by (8.2).

q.e.d.

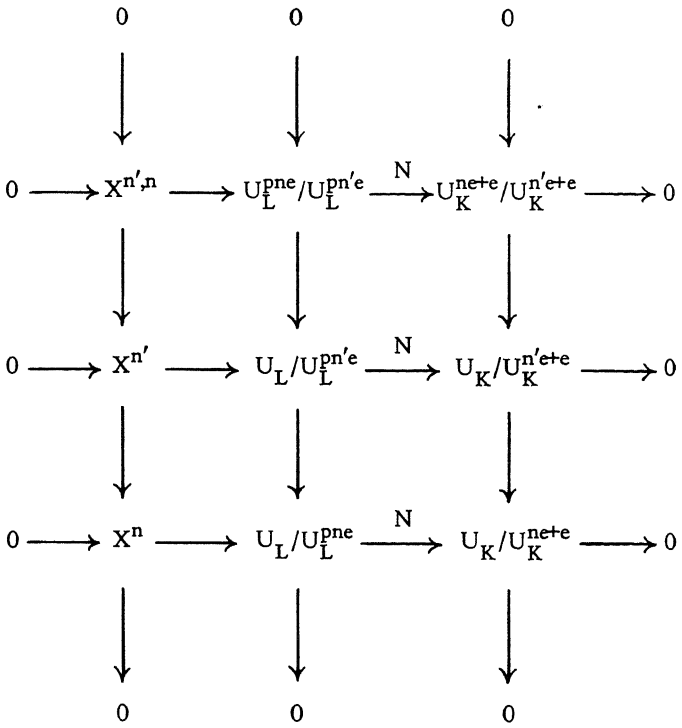
(8.5.D) *Proposition*

Suppose that K contains the p–th roots of unity. Let $L = K(x)$ where x is a root of $X^p - \pi_K$. Then dim (Lie X_{inf}) = ∞.

Proof. In this case we have $t = \frac{pe}{p-1}$ (2.2.B) and (2.5.B.1). From (8.1.4) we obtain $N(U_L^{pne}) = U_K^{ne+e}$. There is an exact sequence

$$0 \to X^n \to U_L/U_L^{pne} \to U_K/U_K^{ne+e} \to 0$$

$A(L)/pA(L)$ has a basis $1, x, \ldots, x^{p-1}$ over $A(K)/pA(K)$. But $\mathrm{Tr}(x^i) = 0$ for $i = 1,\ldots,(p-1)$ and $\mathrm{Tr}(A(K)/pA(K)) = 0$. The map Lie N: Lie $U_L/U_L^{nep} \to$ Lie $U_K/U_K^{e(n+1)}$ is therefore the zero map. (one can also use (8.1.1) to show directly that $\mathrm{Tr}(A(L)) \subset pA(K)$). We find dim X^n = pne – (n+1)e; dim(Lie X^n) = pne; hence dim(Lie $(X^n)_{inf}$) = (n+1)e. If $n' > n$ we have an exact diagram



Lie N = 0 in all three rows. Therefore dim(Lie $(X^{n',n})_{inf}$ = $(n'-n)e$. The sequence $0 \to$ Lie $X^{n',n} \to$ Lie $X^{n'} \to$ Lie $X^{n} \to 0$ is always left exact; by counting dimensions we see that it is also right exact. It follows that Lie $(X^{n'})_{inf} \to$ Lie $(X^{n})_{inf}$ is surjective for all $n' > n$.

Whence dim Lie$(X_{inf}) \geqslant$ dim Lie $(X^{n})_{inf} = (n+1)e$ for all n.

q.e.d.

CHAPTER III

MAXIMAL ABELIAN EXTENSIONS OF LOCAL FIELDS WITH FINITE RESIDUE FIELD

(LOCAL CLASS FIELD THEORY)

The first section (§ 9) of this chapter sketches the relation between Ch. II and Ch. III. Except for this paragraph, of which nothing is needed in the sequel, this chapter is independant of Ch. II and of § 3, 4 of Ch. I (Lemma (3.1) excluded).

In § 10 an isomorphism $U(K)/N_{L/K}U(L) \xrightarrow{\sim} G(L/K)$ is constructed for each totally ramified abelian L/K, and some properties of these isomorphisms are proved. Next, in § 11, we construct (for a given choice of π_K) for each $n \in \mathbf{N}$ a totally ramified abelian extension L_n/K (the so-called Lubin-Tate extensions, cf. (11.2)) and prove that $(\cup L_n . K_{nr}) = K^{ab}$. We then use this to construct an isomorphism

$$\tilde{K}^* = U(K) \times \hat{\mathbf{Z}} \simeq G(K^{ab}/K)$$

such that the kernel of

$$K^* \hookrightarrow \tilde{K}^* \simeq U(K) \times \hat{\mathbf{Z}} \simeq G(K^{ab}/K) \to G(L/K)$$

is exactly $N_{L/K}L^*$ for each abelian L/K. (Because $K^* \simeq U(K) \times \mathbf{Z}$, there is a natural inclusion $K^* \hookrightarrow \tilde{K}^*$). This isomorphism, then, looks remarkably like the 'classical' reciprocity isomorphism, defined by the norm residue symbol, and in fact it is identical with the latter (cf. (11.4.B) Remark 2; this fact is not used further on). As a corollary we then obtain for instance the existence theorem of local class field theory (11.4.D). All this is done without anywhere using the norm residue symbol (cf. [LT] and [19]).

9. THE LANG ISOMORPHISM.

This section serves to point out the link between the considerations of Ch. II and the following two sections (§10,11).

Let U be a (pro-)algebraic group scheme over a field k consisting of q elements.

For each k-algebra A we have a k-algebra homomorphism F: $A \to A$, $a \mapsto a^q$; these induce maps $U(A) \to U(A)$, which define an endomorphism F^U: $U \to U$, the Frobenius endomorphism of U. (We shall usely simply write F instead of F^U). The endomorphisms F are endomorphisms of (pro-) algebraic group schemes and they commute with every homomorphism of group schemes (cf. the remark below).
The F become automorphisms in the category $\mathrm{Pro}(CQG_k)$.
We also use F to denote the canonical generator of the galois group $G(k_s/k)$ (given by $x \mapsto x^q$, $x \in k_s$) and its lift in $G(K_{nr}/K)$, the canonical generator of $G(K_{nr}/K)$, characterized by $F(x) \equiv x^q \bmod \mathfrak{m}(K_{nr})$, for $x \in A(K_{nr})$). Note that the homomorphism F: $U(k_s) \to U(k_s)$, derived from the Frobenius endomorphism of U, is identical with the homomorphism F: $U(k_s) \to U(k_s)$ induced by the action of the galois group $G(k_s/k)$ on $U(k_s)$. It follows from (5.1.A) that both these homomorphisms F: $U(k_s) \to U(k_s)$ are identical with the homomorphism F: $U_K(k_s) \simeq U(\hat{K}_{nr}) \to U(\hat{K}_{nr}) \simeq U_K(k_s)$, obtained restricting $F \in G(K_{nr}/K)$ to $U(\hat{K}_{nr})$, when $U = U_K$ is the pro-algebraic group scheme of units of a local field K with residue field k.

Remark.

The existence of endomorphisms F^U for all (pro-) algebraic group schemes U over k, with the commutation properties mentioned above, is an instance of a much more general situation. Let **C** be any category; and let F be a functor endomorphism of the identity functor. The morphism F induces a functor endomorphism F^T: $T \to T$ for each functor T: $\mathbf{C} \to$ Ens. (Defined by $F^T(A) := T(F(A))$, $A \in \mathbf{C}$). The F^T have the property that $\varphi \circ F^T = F^{T'} \circ \varphi$ for every functor morphism φ: $T \to T'$. In particular, as $F^{T \times T} = F^T \times F^T$, this implies that F^T is an endomorphism of group functors when T is a group functor (and that the F commute with homomorphisms of group functors). If we take $\mathbf{C} = \mathrm{Al}_k$ (= the category of k-algebras) and for T the functor $A \mapsto U(A)$, where U is a (pro-) algebraic group scheme, we obtain the situation described above.

(9.1) **Isogenies with constant kernel.**

Let f: $U_f \to U$ be an isogeny of algebraic group schemes over k with constant kernel K_f (where the field k is supposed to be finite). For $x \in U(k)$, let $x' \in U_f(k_s)$ be a lift of x; then $f(F(x')-x') = fF(x')-f(x') = F(x)-x = 0$ because $x \in U(k)$. The element $F(x') - x'$ does not depend on the choice of x'. For, let x'' be any other lift of x, then $x'' - x' \in K_f(k_s) = K_f(k)$ and therefore $F(x''-x') = x'' - x'$. We have

so defined a homomorphism $U(k) \to K_f(k)$. The image of $x \in U(k)$ in $K_f(k)$ is zero iff we can find a lift $x' \in U_f(k_s)$ such that $F(x') = x'$; i.e. such that $x' \in U_f(k)$. We have:

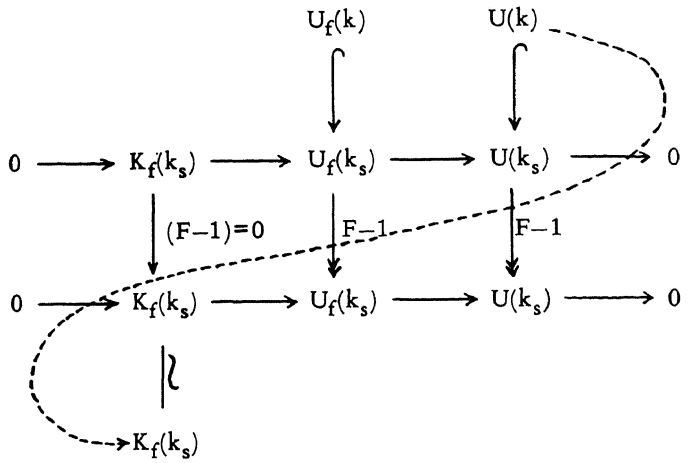
Proposition (Lang)

> If $f: U_f \to U$ is an isogeny of connected algebraic group schemes over k with constant kernel K_f, then the homomorphism $U(k) \to K_f(k)$ described above, induces an isomorphism
>
> $$U(k)/f\,U_f(k) \simeq K_f(k)$$

(This is proved by the above, except for the surjectivity of $U(k) \to K_f(k)$, which follows from the fact that $F-1: U_f(k_s) \to U_f(k_s)$ is surjective for connected algebraic group schemes U_f.)

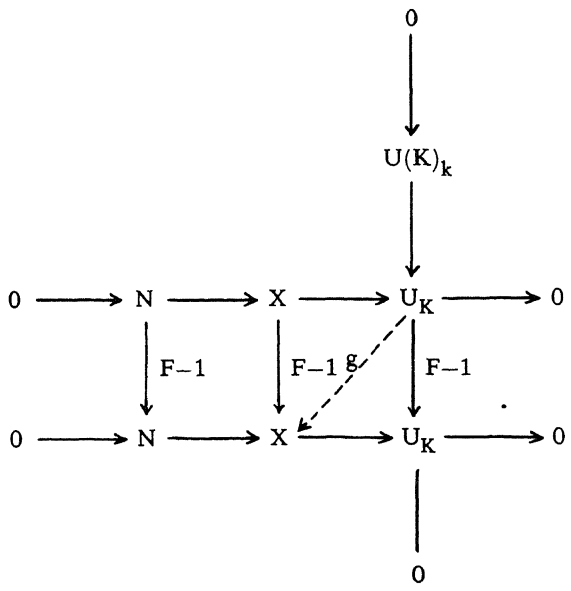
Remark.

We have in fact applied the snake lemma to the exact diagram



(9.2) **The group $\pi(U_K)(k_s)$ when the residue field is finite.**

Let $0 \to N \to X \to U_K \to 0$ be an isogeny with constant kernel of the pro-algebraic group scheme U_K of units of the local field K with finite residue field k ($\#k = q$). Consider the exact diagram



(For the fact that F−1: $U_K \to U_K$ is epimorphic cf. (10.1.A)). The constant group scheme $(U(K))_k$ is pro-finite (because k is finite). The morphism F−1 is zero on N because N is constant, therefore $N \to X \xrightarrow{F-1} X$ is zero; it follows that there exists a morphism g as indicated in the diagram which factorizes F−1: $U_K \to U_K$ through X. The isogeny F−1: $U_K \to U_K$ is hence larger than all isogenies with constant kernel of U_K. It follows that

$$\pi(U_K) \simeq U(K)_k, \quad \pi(U_K)(k_s) \simeq U(K) \tag{9.2.1}$$

and by applying theorem (5.4.D) that

$$G(K^{ab}/K)_{ram} \simeq \sigma_K \simeq U(K). \tag{9.2.2}$$

This last isomorphism will be established again in § 10, 11, but then without using algebraic geometry.

(9.3) **Description of the isomorphism** (9.2.2).

It was Serre in section 7 of [17] who remarked that the Lang isomorphism (9.1) (or rather its pro-algebraic analogue) should be the think between the theory of chapter II and the 'classical' class field theory of local fields with finite residue field.

Let L/K be a totally ramified abelian extension of the local field K with finite residue field k. We have an isogeny with constant kernel over k (cf. (5.2.B)).

$$0 \to (G(L/K))_k \to U_L/V_L \xrightarrow{N_{L/K}} U_K \to 0$$

From this we obtain an isomorphism (9.1)

(9.3.1) $$U_K(k)/N_{L/K}(U_L/V_L(k)) \simeq G(L/K)$$

One now proves that $N_{L/K}(U_L/V_L(k)) = N_{L/K}(U(L))$ (cf. (10.2); we know that $U(K) \simeq U_K(k)$), and we find an isomorphism

(9.3.2) $$\varphi\colon U(K)/N_{L/K}(U(L)) \xrightarrow{\sim} G(L/K)$$

(cf. also (10.2), where this isomorphism is constructed again)

We showed in (5.1.A) that the action of $G(k_s/k)$ on $U_k(k_s) \simeq U(\hat{K}_{nr})$ is the same as the action of $G(k_s/k) \simeq G(K_{nr}/K)$ on $U(\hat{K}_{nr})$ as a subset of $A(\hat{K}_{nr})$. Let F be the Frobenius automorphism in $G(K_{nr}/K)$, then $u \in U_K(k) \simeq U(K)$ iff $(F-1)(u) = 0$. The recipe for the isomorphism φ of (9.3.2) now becomes:

> take $u \in U(K)$, let $u' \in U(\hat{L}_{nr})$ be any lift of u; then there is exactly one $\varphi(u) \in G(L/K)$ such that
>
> $$\frac{\varphi(u)(\pi_L)}{\pi_L} \equiv \frac{Fu}{k'} \text{ mod. } V(\hat{L}_{nr})$$
>
> the isomorphism φ is induced by the homomorphism
>
> $$u \mapsto \varphi(u)$$

If we had taken instead of $u \mapsto \varphi(u)$, the homomorphism $u \mapsto \varphi(u^{-1})$, we would have obtained exactly the description of the reciprocity isomorphism for totally ramified abelian extensions given by Dwork in [4] (cf. also [CL] Ch. XIII § 5 (especially the Cor. to Th. 2 and p. 210) and (11.4.B) Remark 2).

10. 'ALMOST' THE RECIPROCITY ISOMORPHISM.

In this and the following section K will be a local field with a finite residue field consisting of q elements. We use the symbol F for the Frobenius automorphism of $G(k_s/k)$ and for the canonical lift of this automorphism in $G(K_{nr}/K)$.

Let L/K be a totally ramified abelian extension of K. In (10.1) we prove some lemmas necessary to define an isomorphism

$$\varphi\colon U(K)/N_{L/K}U(L) \simeq G(L/K)$$

in (10.2) for abelian totally ramified extensions L/K. The isomorphism φ (or more precisely the isomorphism $u \mapsto \varphi(u^{-1})$) will play an important part in the definition of the reciprocity isomorphism in (11.4.B). In (10.3) we note a functorial property of this isomorphism.

(10.1) **Some lemmas.**

(10.1.A) *Lemma*

The homomorphisms $F-1\colon U(\hat{L}_{nr}) \to U(\hat{L}_{nr})$ and $F-1\colon V(\hat{L}_{nr}) \to V(\hat{L}_{nr})$ are surjective. $((F-1)(u) := \frac{Fu}{u}$ if we write the groups $U(\hat{L}_{nr})$ and $V(\hat{L}_{nr})$ multiplicatively).

Proof. Use the filtration by the $U^n(\hat{L}_{nr})$ of $U(\hat{L}_{nr})$. The induced homomorphisms are $U(\hat{L}_{nr})/U^1(\hat{L}_{nr}) \simeq k_s^* \to k_s^* \simeq U(\hat{L}_{nr})/U^1(\hat{L}_{nr})$, $x \mapsto x^{q-1}$ and for $i \geqslant 1$ $U^i(\hat{L}_{nr})/U^{i+1}(\hat{L}_{nr}) \simeq k \to k \simeq U^i(L_{nr})/U^{i+1}(L_{nr})$, $x \to x^q - x$ (Note that k_s is written additively). These homomorphisms are all surjective (as k_s is algebraically closed). An application of lemma (3.1) yields the first part of the lemma.

Let $\frac{tx}{x} \in V(\hat{L}_{nr})$ $t \in G(L/K)$ (these elements generate $V(\hat{L}_{nr})$); choose $y \in U(\hat{L}_{nr})$ such that $(F-1)(y) = x$; then we have

$$(F-1)\left(\frac{ty}{y}\right) = \frac{Fty}{Fy}\Big/\frac{ty}{y} = \frac{tFy}{ty}\Big/\frac{Fy}{y} = t\left(\frac{Fy}{y}\right)\Big/\frac{Fy}{y} = \frac{tx}{x}$$

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

q.e.d.

(10.1.B) *Lemma.*

Suppose $Fx = x$ for $x \in \hat{K}_{nr}$, then $x \in K$.

Proof. Write $x = \pi_K^n u$, $u \in U(\hat{K}_{nr})$, $\pi_K \in K$; $Fx = x$ yields $Fu = u$; write $u = u_0' + \pi_K w_1'$ with $u_0' \in K_{nr}$; $Fu = u$ yields $Fu_0' = u_0'$ mod. π_K; hence we can write $u = u_0 + \pi_K w_1$ with $u_0 \in K$; then $Fu = u$ yields $Fw_1 = w_1$; repeating this proces with w_1 we obtain $u = u_0 + \pi_K u_1 + \pi_K^2 w_2$, $u_0, u_1 \in K$. Continuing in this way

we see that $u \in K$ mod. π_K^n for all n, and hence that $u \in K$ and $x \in K$ because K is complete.

q.e.d.

(10.1.C) *Remark.*

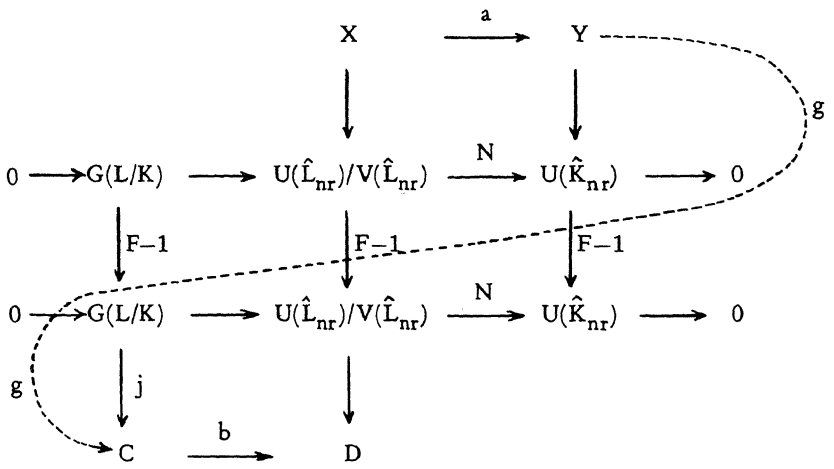
Let $\hat{\Omega}$ be a completion of an algebraic closure Ω of K. The galois group $G(\Omega/K)$ acts on $\hat{\Omega}$ (extend the action of $G(\Omega/K)$ on Ω by continuity). In this case also we have for all $x \in \hat{\Omega}$

$$(sx = x \text{ for all } s \in G(\Omega/K)) \Leftrightarrow x \in K.$$

The proof of this (cf. [20] (3.3) Th. 1) is much more difficult because the valuation on $\hat{\Omega}$ is no longer discrete.

(10.2) **'Almost' the reciprocity isomorphism.**

Let L/K be a totally ramified abelian extension. Consider the following exact diagram (cf. (2.7.A.2) and (9.1) Remark)



X, Y, C and D are the respective kernels and cokernels of the vertical maps in the middle.

(i) By the snake lemma ([2] § 1.4 Prop. 2) there exists a homomorphism g: $Y \to C$ such that the sequence $X \to Y \to C \to D$ is exact.

(ii) The homomorphism j is an isomorphism. For $F\left(\frac{s\pi_L}{\pi_L}\right) = \frac{Fs\pi_L}{F\pi_L} = \frac{sF\pi_L}{F\pi_L} \equiv \frac{s\pi_L}{\pi_L}$

mod. $V(\hat{L}_{nr})$ which proves that F−1 is zero on G(L/K) (cf. also (2.7.A.3) and (5.1.C)).
(iii) Y = U(K) according to Lemma (10.1.B).
(iv) The homomorphism b is zero. For F−1: $U(\hat{L}_{nr}) \to U(\hat{L}_{nr})$ is surjective (10.1.A); i.e. D = 0.
(v) $a(X) = N_{L/K}U(L)$. It is clear that $N_{L/K}U(L) \subset a(X)$; let $\overline{x} \in X$ be represented by $x \in U(\hat{L}_{nr})$, then Fx/x is in $V(\hat{L}_{nr})$, by lemma (10.1.A) there exists an $y \in V(\hat{L}_{nr})$ such that F(y)/y = F(x)/x, then $F(xy^{-1}) = xy^{-1}$, hence $xy^{-1} \in U(L)$ (10.1.B); and $N_{L/K}(xy^{-1}) = N(x) = N(\overline{x}) = a(\overline{x})$.
(i)–(v) imply that the homomorphism

$$\varphi\colon U(K)/N_{L/K}(U(L)) \xrightarrow{\sim} G(L/K)$$

induced by g is an isomorphism.

Remarks.

1. Dwork has shown in [4] that the isomorphism $u \mapsto \varphi(u^{-1})$ is in fact the 'classical' reciprocity isomorphism. (Cf. the last few lines of § 9).
2. Also when the residue field k of K is quasi-finite (instead of finite) one can prove that the homomorphism φ is an isomorphism. The proof has to be changed slightly because in this case F−1: $U(\hat{L}_{nr}) \to U(\hat{L}_{nr})$ is not necessarily surjective. We have instead:

$$(x \equiv \text{root of unity mod. } U^1(L_{nr})) \Rightarrow (x \in \mathrm{Im}(F-1)).$$

   This suffices to prove that b = 0.
3. If we take an arbitrary finite abelian extension L/K and for F in the middle column of the diagram any lift F′ in $G(L_{nr}/K)$ of the canonical generator of $G(k_s/k)$, then we obtain in exactly the same way

$$G(L/K)_{ram} \simeq U(K)/N_{L'/K}U(L')$$

   (replace G(L/K) by $G(L/K)_{ram}$ in the diagram), where L′ is the invariant field of F′. Therefore, because $N_{M'/M}(U(M)) = U(M)$ if the extension M′/M is unramified (2.6.J), we see that

$$G(L/K)_{ram} \simeq U(K)/N_{L/K}U(L)$$

   also in this case.
4. Let L/K be a not necessarily abelian totally ramified galois extension, then we obtain an isomorphism

$$G(L/K)^{ab} \simeq U(K)/N_{L/K}U(L)$$

The proof is exactly the same, except that we must replace $G(L/K)$ by $G(L/K)^{ab}$ in the diagram above (cf. (2.7.A.2)).

5. Let L/K be any galois extension. Let $H := G(L/K)_{ram}$. Then we can construct exactly the same diagram as above with H^{ab} instead of $G(L/K)$. (For F in the middle column take any lift in $G(L_{nr}/K)$ of $F \in G(K_{nr}/K)$), cf. Remark 3 above). The homomorphism $F-1: H^{ab} \to H^{ab}$ is then not necessarily zero. Its cokernel is the quotient $H/\langle G,H\rangle$ of $H^{ab} := H/\langle H,H\rangle$ (where $G = G(L/K)$) Cf. (5.2.D). We find an isomorphism

$$H/\langle G,H\rangle \xrightarrow{\sim} U(K)/N_{L/K}U(L).$$

(Again with the help of (2.6.J) as in Remark 3. Cf. also (5.2.D).)

(10.3) **Functoriality**

The isomorphism φ described above is functorial in L. I.e. if M/K is a larger totally ramified extension than L/K (in the sense that $M \supset L$; or even in the sense of $M_{nr} \supset L_{nr}$, cf. (2.8.H)) then the following diagram is commutative.

$$\begin{array}{ccc} G(M/K) & \xleftarrow{\sim} & U_K/N_{M/K}U(M) \\ \downarrow & & \downarrow \\ G(L/K) & \xleftarrow{\sim} & U_K/N_{L/K}U(L) \end{array}$$

(Both the vertical homomorphisms are the natural projections). The commutativity follows from the functoriality of the fundamental exact sequence (2.7.A.2) (cf. also (5.3)) and the functoriality of the snake lemma.

11. LOCAL CLASS FIELD THEORY.

In this section as in the preceding one K is a local field with a finite residue field consisting of q elements. We here use π (instead of π_K) to denote a uniformizing element of K.

Let $f \in F_\pi$ be a Lubin-Tate power series (cf. (2.2)); i.e.

$$f \equiv \pi X \bmod. X^2 \quad \text{and} \quad f \equiv X^q \bmod. \pi$$

Let λ_m be a root of $f^{(m)}$ but not of $f^{(m-1)}$ (we denote with $f^{(m)}$ the m-th iterate of f; i.e. $f^{(m)} := f^{(m-1)} \circ f$, $f^{(1)} := f$). Define $L_m := K(\lambda_m)$ and $L_\pi = \cup L_m$. When $K = \mathbf{Q}_p$, for instance, we might take $f := (1+X)^p - 1$, then $f^{(m)} = (1+X)^{p^m} - 1$, and $L_m = K(\zeta_p m)$ where $\zeta_p m$ is a primitive p^m-th root of unity. It is well known that in this case $\mathbf{Q}_p^{ab} = L_p.(\mathbf{Q}_p)_{nr}$. The first three sections ((11.1)–(11.3)) establish the analogous fact (that $L_\pi.K_{nr} = K^{ab}$) when K is any local field with a finite residue field (consisting of q elements) and f is a Lubin-Tate polynomial of degree q. To this end we show in section (11.1) that the extensions L_m/K have small norm groups (in fact that $N_{L_m/K}U(L_m) \subset U^m(K)$), and in (11.2) that the L_m/K are normal abelian totally ramified extensions. (This is done without using formal groups). In section (11.3) we calculate $\sigma_K = G(K^{ab}/K)_{ram}$ and show that indeed $K^{ab} = L_\pi.K_{nr}$. We then use this in (11.4) to define a reciprocity homomorphism (injective)

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

such that the kernel of

$$K^* \to G(K^{ab}/K) \to G(L/K)$$

is precisely $N_{L/K}(L^*) \subset K^*$ for every abelian L/K.
One can also base the construction of the reciprocity isomorphism in (11.4) on (9.2) instead of on (11.3.A).

(11.1) **Construction of extensions with small norm groups.**

(11.1.A) *Lemma*

> Let k be an arbitrary field, $g = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ 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 $\leqslant r-1$ such that the polynomial $h := X^r g + \tilde{g}$ is separable (i.e. has only simple roots).

Before proving this lemma we want to state a corollary (which is equivalent with the lemma). Give the multiplicative group $M_k := 1 + X\,k[[X]]$ of power series in X over k with constant term equal to 1 the topology induced by the system of open subgroups $1 + X^n\,k[[X]]$.

Corollary. The separable polynomials $1 + a_1X + \ldots + a_nX^n$ are dense in the topological group M_k.

PROOF OF THE LEMMA.

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 $\frac{dg}{dX} \not\equiv 0$ (because (n, 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 ($r = q^{s+1}$; $\tilde{g} := -X^q g(X) + 1$)

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

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.

Let f be a polynomial over A(K) of type (Lubin-Tate polynomial)

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

We use $f^{(m)}$ to denote the m-th iterate of f, i.e. $f^{(m)} := f(f^{(m-1)})$, $f^{(1)} = f$. As X divides f, it follows that $f^{(m-1)}$ divides $f^{(m)}$. One sees directly from the shape of f that $f^{(m)}/f^{(m-1)}$ is an Eisenstein polynomial. Let λ_m be a root of this Eisenstein polynomial and let $L_m := K(\lambda_m)$. The extension L_m/K is totally ramified of degree $(q-1)q^{m-1}$. We can choose the λ_m inductively in such a way that $f(\lambda_m) = \lambda_{m-1}$, then $L_{m-1} \subset L_m$ and we can form $L_\pi := \bigcup_m L_m$.

(11.1.B) *Theorem*

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

Proof. Every element of $U(L_m)$ can be written as u u′ with u′ a (q-1)-th root of unity in K and $u \in U^1(L_m)$. Now $N(u') = (u')^{(q-1)q^{m-1}} = 1$. 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 $m \geqslant 2$. 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 $v(x) \geqslant v(\pi^m)$, so that (n, char(k)) = 1 (as $m \geqslant 2$; 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 the lemma (11.1.A),

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 $v(x') \geqslant v(\pi^m)$ and $u = 1 + a_1\lambda + \ldots + a_n\lambda^n + x = (1-z_1\lambda) \ldots (1-z_t\lambda)(1+y)$ with $v(y) \geqslant v(\pi^m)$. 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).

(11.1.B.1)

$$\begin{array}{ccc} L_m & \hookrightarrow & L_m.K_{nr} \\ \Big\downarrow N = N_{L_m/K} & & \Big\downarrow N_{L_m.K_{nr}/K_{nr}} \\ K & \hookrightarrow & K_{nr} \end{array}$$

(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 $f^{(m)}/f^{(m-1)} \in K_{nr}[X]$. This yields

$$(11.1.B.2) \qquad N(1-z\lambda) = z^{(q-1)q^{m-1}} \frac{f^{(m)}(z^{-1})}{f^{(m-1)}(z^{-1})} \qquad z \in U(K_{nr})$$

(Thanks to the commutativity of the diagram (11.1.B.1) above we can and shall use N for both $N_{L_m/K}$ and $N_{L_m.K_{nr}/K_{nr}}$ indiscriminatedly).
Putting $y_i := z_i^{-1}$ we obtain from (11.1.B.2)

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

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

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

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

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

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

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

because also $x \mapsto f(x)$ reduces to $x \mapsto x^q$ mod. (π).
For any two elements $a, b \in A(K_{nr})$, if $a \equiv b$ mod. (π^r) with $r \geqslant 1$ then $a^q \equiv b^q$ mod. (π^{r+1}) and $\pi a^s \equiv \pi b^s$ mod. (π^{r+1}) $(s = 1, \ldots, q-1)$ hence also $f(a) \equiv f(b)$ mod. (π^{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

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

q.e.d.

Remark. Note that the first part of the proof above shows that:
The unramified polynomials $1 + a_1 X + \ldots + a_n X^n$ are dense in the topological group $1 + X A(K)[[X]]$.

(11.2) The Lubin-Tate extensions.

Consider the polynomial $f := X^q + \pi X$; f is of the type discussed in the preceding section. By the fundamental Lubin-Tate lemma (2.2.A) there exists for every $a \in A(K)$ exactly one power series $[a]_f$ such that

$$[a]_f \equiv aX \text{ mod. } X^2 \quad \text{and} \quad f \circ [a]_f = [a]_f \circ f.$$

As in the preceding section let $L_m = K(\lambda_m)$ where λ_m is a root of $f^{(m)}$ but not a root of $f^{(m-1)}$. For every $u \in U(K)$ we obtain (possibly) another root $[u]_f(\lambda_m) \in L_m$ of $f^{(m)}$ which is not a root of $f^{(m-1)}$. It is our aim to prove in this section that L_m/K is an abelian totally ramified extension for every $m \geqslant 1$. This is done by showing that one finds enough different roots $[u]_f(\lambda_m) \in L_m$ when u runs through U(K). To do this we need to know somewhat more about the power series $[u]_f$. This can be found by direct calculation as in (11.2.A) and (11.2.B) or by a more elegant method (11.2.C) and (11.2.D) for the suggestion of which I am indebted to A. Menalda.

(11.2.A) *Lemma.*

Let $f := X^q + \pi X$. If $u = 1 + \pi^n x$, $x \in U(K)$, then we have for the power series $[u]_f = u_1 X + u_2 X^2 + \ldots$

$$\begin{aligned}
&v(u_1) = 0;\ v(u_i) \geqslant n && i = 2, \ldots, q-1\\
&v(u_q) = n-1;\ v(u_i) \geqslant n-1 && i = q+1, \ldots, q^2-1\\
&v(u_{q^2}) = n-2;\ v(u_i) \geqslant n-2 && i = q^2+1, \ldots, q^3-1\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&v(u_{q^n}) = 0
\end{aligned}$$

Proof. $u(X^q + \pi X) \equiv (uX)^q + \pi uX$ mod. X^q. Therefore $u_1 = u$ and $v(u_1) = 0$ and $u_2 = u_3 = \ldots = u_{q-1} = 0$. The coefficient u_q must be equal to $(u^q-u)/(\pi^q-\pi)$ hence $v(u_q) = n-1$ if $n \geqslant 1$. Suppose we have proved the lemma for $i \leqslant q^m$, $1 \leqslant m < n$. Consider the coefficient of X^{q^m+j} for $1 \leqslant j \leqslant (q-1)q^m$ in the relation

$$[u]_f(X^q + \pi X) = [u]_f^q + \pi[u]_f$$

The coefficient of X^{q^m+j} on the left side is

$$u_{n'}\pi^{n'} + \binom{n'-(q-1)}{1} u_{n'-(q-1)}\pi^{n'-q} + \binom{n'-2(q-1)}{2} u_{n'-2(q-1)}\pi^{n'-2q} + \ldots \binom{n'-t(q-1)}{t} u_{k+t}\pi^k$$

where $k := q^m + j - tq$, $t := \left[q^{m-1} + \frac{j}{q} \right]$, $n' := q^m + j$.

One has $k = 0$ if $(q,j) = q$ and $k > 0$ elsewhere. Assume the lemma proved for indices smaller than n'. Then we know that

$$[u]_f \equiv uX + \pi^{n-m} \text{ (something) } \text{ mod. } (X^{n'})$$

therefore

$$[u]_f^q \equiv u^q X^q + \pi^{n-m+1} \text{ (something) } \text{ mod. } (X^{n'+1})$$

We therefore have the relation

$$(11.2.A.1) \quad u_{n'}\pi^{n'} + \binom{n'-(q-1)}{1} u_{n'-(q-1)}\pi^{n'-q} + \ldots + \binom{n'-t(q-1)}{t} u_{k+t}\pi^k = \\ = \pi^{n-m+1}y + \pi u_{n'}$$

If $k > 0$, we obtain $v(u_{n'}) \geqslant \min(n-m+1, v(u_{k+t}) + 1) - 1 \geqslant n-m$.
If $k = 0$ and $1 \leqslant j < (q-1)q^m$ we obtain $v(u_{n'}) \geqslant \min(n-m+1, v(u_t)) - 1 \geqslant n-m$.
If $k = 0$ and $j = (q-1)q^m$ we have $t = q^m$ and $v(u_t) = n-m$; the coefficient of u_t in the relation above is then 1, the term u_t has in this case strictly smaller value than all the others on the left, therefore we have exactly $v(u_{n'}) = v(u_t) = n-m-1$.

q.e.d.

(11.2.B) *Lemma.*

Let $f := X^q + \pi X$ and λ_m as above. If $[u]_f(\lambda_m) = [u']_f(\lambda_m)$ then $u \equiv u'$ mod. $U^m(K)$.

Proof. Composing with $[u^{-1}]_f$ we obtain $[u^{-1}u']_f(\lambda_m) = \lambda_m$ and we have to prove $u^{-1}u' \in U^m(K)$ (cf. the remark below). Suppose then that $[u]_f(\lambda_m) = \lambda_m$. We proceed by induction. The case $m = 1$ is clear. As $[u]_f(\lambda_{m-1}) = [u]_f(f(\lambda_m)) = f([u]_f(\lambda_m)) = f(\lambda_m) = \lambda_{m-1}$ we know by the induction hypothesis that $u \in U^{m-1}(K)$, i.e. $u = 1 + \pi^{m-1}x$. Suppose $v(x) = o$ (i.e. $u \in U^{m-1}(K) \setminus U^m(K)$) then $v(u_{q^{m-1}}) = 0$ by the preceding lemma. The value of all terms of $[u]_f(\lambda_m) - \lambda_m$, except $u_{q^{m-1}} \lambda_m^{q^{m-1}}$, is $\geqslant (q^{m-1} + 1)\, v(\lambda_m)$, because $v(\pi) = (q-1)q^{m-1}v(\lambda_m)$. This gives a contradiction, hence $v(x) > 0$ and $u \in U^m(K)$.

q.e.d.

Remark.

The fact that $[u]_f([u']_f) = [uu']_f$ used in (11.2.B) and (11.2.E) further on, follows from the uniqueness property of the series $[\ ]_f$; both right hand and left hand side start off with $uu'X + \ldots$ and both commute with f, therefore they are equal (2.2.A).

(11.2.C) *Proposition.*

> Let f be a power series over A(K) (no hypothesis on the residue field of K). Suppose $\lambda \in L$ (where L/K is a finite extension) is a root of positive value of f (i.e. $v(\lambda) > 0$). Then there exists a power series g with coefficients in A(L) such that $f = (X-\lambda)\, g$.

Proof. Write $f \equiv (X-\lambda)\, g_n + h_n \bmod (X^n)$, with $h_n \in A(L)$ (division with remainder in $A(L)[X]$). Now $f(\lambda) = 0$, therefore $v(h_n) \geqslant n\, v(\lambda)$ which goes to infinity as $n \to \infty$ because $v(\lambda) > 0$. Also we have $f \equiv (X-\lambda) g_{n+1} + h_{n+1} \bmod X^{n+1}$, therefore $(X-\lambda)(g_{n+1}-g_n) \equiv 0 \bmod (\lambda^n, X^n)$. We write $g_{n+1} - g_n = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$, and we obtain

$$v(a_0\lambda) \geqslant nv(\lambda),\ v(a_1\lambda - a_0) \geqslant nv(\lambda), \ldots, v(a_{n-1}\lambda - a_{n-2}) \geqslant nv(\lambda)$$

from which

$$v(a_0) \geqslant (n-1)\, v(\lambda),\ v(a_1) \geqslant (n-2)\, v(\lambda), \ldots, v(a_{n-1}) \geqslant 0.$$

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

q.e.d.

(11.2.D) SECOND PROOF OF (11.2.B).

As in (11.2.B) we have to prove that $[u]_f(\lambda_m) = \lambda_m$ implies $u \equiv 1 \bmod \pi^m$. Let $s \in G(K, L \to \Omega)$, then also $s\lambda_m$ is a root of $[u]_f(X) - X$ because of the continuity of the action of s. Also $f^{(r)}(\lambda_m)$ is a root of $[u]_f(X) - X$ because $[u]_f$ commutes with f and $f(0) = 0$. Therefore all the roots of $f^{(m)}$ are roots of $[u]_f(X) - X$. By repeated application of (11.2.C) we obtain a factorisation

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

But $f^{(m)} = \pi^m X + \ldots$; comparing the coefficients of X left and right we find $(u-1) = \pi^m a$ for some a with non negative value.

q.e.d.

Remarks.

1. For this second proof of (11.2.B) we did not need to suppose that $f = X^q + \pi X$ but only that f is of the shape

$$f = X^q + \pi(a_{q-1}X^{q-1} + \ldots + a_2X^2) + \pi X.$$

2. One can also give a proof of (11.2.B) analogous to (11.2.D) in the case that f is a Lubin-Tate *power series.*

(11.2.E) *Theorem.*

The extensions L_m/K are galois extensions with galois group isomorphic to $U(K)/U^m(K)$.

Proof. $\#U(K)/U^m(K) = (q-1)q^{m-1} = [L_m : K]$. With λ_m also $[u]_f(\lambda_m) \in L_m$ and these elements are all roots of $f^{(m)}$ and not of $f^{(m-1)}$ if $u \in U(K)$. In this way we obtain in virtue of (11.2.B) at least $\#(U(K)/U^m(K)) = (q-1)q^{m-1}$ different roots of $f^{(m)}/f^{(m-1)}$ in L_m. This proves that L_m/K is normal. The extension L_m/K is separable as it is a composite of extensions $L_m \supset L_{m-1} \supset \ldots \supset L_1 \supset K$, defined by polynomials $X^q + \pi X - \lambda_m$, $X^{q-1} + \pi$. (Or, L_m/K is defined by a polynomial of degree $(q-1)q^{m-1}$ with no multiple roots). The assignment $s \mapsto$ (class of any u such that $s(\lambda_m) = [u]_f(\lambda_m)$) defines the desired isomorphism $G(L_m/K) \xrightarrow{\sim} U(K)/U^m(K)$. That this map is an homomorphism follows from (2.2.A). Cf. the remark below (11.2.B).

q.e.d.

(11.2.F) *Corollary*

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

Proof. We now from (11.1.B) that $N_{L_m/K}(U(L_m)) \subset U^m(K)$. As both groups have index $q^{m-1}(q-1)$ in $U(K)$, the corollary follows (10.2).

q.e.d.

(11.2.G) *Remark.*

The element $\pi \in K$ is a norm from every L_m/K.

Proof. We defined L_m as $L_m = K(\lambda_m)$ where λ_m is a root of $f^{(m)}/f^{(m-1)}$. This polynomial is of the shape $X^{(q-1)q^{m-1}} + \pi(\ldots) + \pi$. It follows that $N_{L_m/K}(-\lambda_m) = \pi$ for all L_m/K with $m \geqslant 1$.

q.e.d.

2.H) *Remark.*

can use (11.2.A) to calculate the ramification groups of $G(L_m/K)$ and the nction of L_m/K. It turns out that $G(L_m/K)_{\psi(i)} = G(L_m/K)^i$ corresponds $U^i(K)/U^m(K)$ under the isomorphism $G(L_m/K) \xrightarrow{\sim} U(K)/U^m(K)$ for $i \leqslant m$; and that $G^i = 0$ when $i \geqslant m$. For the ψ-function we find

$$\psi(i) = q^i - 1 \qquad i \leqslant m$$
$$\psi(i) = (q^m - 1) + (i-m)(q^m - q^{m-1}) \qquad i \geqslant m$$

3) **Calculation of α_K. Description of K^{ab}.**

3.A) *Theorem*

$$\alpha_K \simeq U(K)$$

of. For every totally ramified abelian extension L/K we have an isomorphism 2), which is functorial

$$\varphi: U(K)/N_{L/K}U(L) \xrightarrow{\sim} G(L/K)$$

every finite quotient G of α_K there exists a totally ramified extension with is group G ((2.8.H); α_K is a galois group; (2.8.F)). Hence taking the pro- ive limit of the isomorphisms above, we find an isomorphism

3.A.1) $$\varphi: \varprojlim_{L/K} U(K)/N_{L/K}U(L) \xrightarrow{\sim} \alpha_K$$

also the definition of the projective system defining α_K (2.8.H) and (2.1.B)) (L) is compact, $N_{L/K}$ is continuous, hence $N_{L/K}(U(L))$ is also compact and herefore closed in U(K); it is also of finite index in U(K) (10.2) and there- ore also open in U(K); i.e. there exists an n such that $U^n(K) \subset N_{L/K}(U(L))$. y (11.1.B) and (11.2.E) there exists for every n a totally ramified abelian xtension L_n such that $N_{L_n/K}(U(L_n)) \subset U^n(K)$.
nd b) together imply that

.3.A.2) $$\varprojlim_{L/K} U(K)/N_{L/K}U(L) \simeq \varprojlim_{n} U(K)/U^n(K) \simeq U(K)$$

mulas (11.3.A.1) and (11.3.A.2) together prove the theorem.

q.e.d.

$L_\pi := \bigcup_m L_m$, where $L_m := K(\lambda_m)$, λ_m a root of $f^{(m)}/f^{(m-1)}$, $f := X^q + \pi X$

(or any other Lubin-Tate power series in F_π; cf. (2.2.A) and (11.2.D) Remark 2). Section (10.2) implies that $G(L_\pi/K) \simeq \varprojlim U(K)/U^n(K) \simeq U(K)$ (cf. also (11.2.F)).

(11.3.B) *Corollary (Description of* K^{ab}*).*

Every abelian extension L/K (in Ω) is contained in the abelian extension $L_\pi.K_{nr}$.

Proof. There exists a totally ramified abelian extension L'/K such that $L.K_{nr} = L'.K_{nr}$ for every abelian extension L/K (2.8.F). There is an n such that $N_{L'/K}(U(L')) \supset U^n(K)$. It follows that $L'.\hat{K}_{nr} \subset L_n.\hat{K}_{nr}$ ((10.3) or (11.3.A); cf. also (11.2.F)) and hence that $L.K_{nr} = L'.K_{nr} \subset L_n.K_{nr}$ ((2.1.C); cf. also the definition of the projective system defining σ_K in (2.8.H)).

q.e.d.

(11.3.C) *Corollary*

$$G(K^{ab}/K) \simeq U(K) \times \hat{\mathbf{Z}}$$

This follows from (11.3.A) together with (2.8.H); or from (11.3.B) directly, as K_{nr} and L_π are linearly disjoint.

(11.3.D) *Remarks.*

1. The group $U(K) \times \hat{\mathbf{Z}}$ is the completion of $K^* \simeq U(K) \times \mathbf{Z}$ 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 $U(K) \times \hat{\mathbf{Z}}$, and $K^* \hookrightarrow \tilde{K}^*$ will be the natural inclusion.
2. One can of course choose many isomorphisms $\tilde{K}^* \simeq U(K) \times \hat{\mathbf{Z}} \simeq G(K^{ab}/K)$. It is the aim of the next section to show that we can choose this isomorphism in such a way that the kernel of

$$K^* \hookrightarrow \tilde{K}^* \to G(K^{ab}/K) \to G(L/K)$$

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

(11.4) The reciprocity isomorphism and the existence theorem.

(11.4.A) PRELIMINARY DEFINITION.

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: $K^* \to G(L'.K_n/K)$ as follows. (Strictly we should write $r_{L'.K_n}$ or something similar).

$$U(K) \ni u \mapsto r(u) := \varphi(u^{-1}) \in G(L'/K) = G(L'.K_n/K_n)$$
$$\pi_K \mapsto F$$

where F is the Frobenius automorphism of $G(L'.K_n/K)$ and $u \mapsto \varphi(u)$ is the homomorphism defined in (10.2).

(11.4.A.1) *Lemma*

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

Proof. 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. (10.2) and (10.2) Remark 3). There is an exact diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U(L) & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \times f} & & \\ 0 & \longrightarrow & U(K) & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbf{Z} & \longrightarrow & 0 \end{array}$$

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

q.e.d.

(11.4.A.2) *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
>
> $$\mathrm{Ker}(K^* \xrightarrow{r} G(L'.K_n/K) \to G(L''/K)) = N_{L''/K}(L''^*).$$

Proof. (11.4.A.1) implies that it suffice to show that $N_{L''/K}(L''^*) \subset \mathrm{Ker}(\dots)$. For this it suffices to show that $N_{L''/K}(\pi'') \in \mathrm{Ker}(\dots)$ when π'' is a uniformizing element of L''. (Because $N_{L''/K}(U(L'')) \subset \mathrm{Ker}(r)$ (10.2), or because the uniformizing elements of L'' generate L''^*). Let L'' be the invariant field of $r(u)F$. Write $\pi'' = x\pi'$ where $\pi' \in L'$ is such that $N_{L'/K}(\pi') = \pi_K$. We have

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

hence $N_{L'.K_n/K_n}(x) \in U(K)$. Now $r(u)F(\pi'') = \pi''$, it follows that we have in the group $U(L'_{nr})$

$$\frac{\varphi(u^{-1})(\pi')}{\pi'} = \frac{r(u)(\pi')}{\pi'} = \frac{x}{r(u)F(x)} = \frac{r(u)F(x^{-1})}{x^{-1}} = \frac{r(u)F(x^{-1})}{F(x^{-1})} \cdot \frac{F(x^{-1})}{x^{-1}} \equiv \frac{F(x^{-1})}{x^{-1}}$$

$$\text{mod. } V(\hat{L}'_{nr}).$$

Hence by the definition of the isomorphism φ in (10.2) $N_{L'.K_n/K_n}(x) = u$ mod. $N_{L'/K}(U(L'))$. And we find

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

which is the identity on L''.

q.e.d.

(11.4.A.3) *Corollary*

If we had defined $r: K^* \to G(L'.K_n/K_n)$ using L'' instead of L', i.e. if we had taken

$$U(K) \ni u \mapsto r(u) := \varphi(u^{-1})$$
$$N_{L''/K}(\pi'') \mapsto F'$$

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

(11.4.A.4) *Remark*

It is clear from the definition of r in (11.4.A) that

$$\mathrm{Ker}(K^* \to G(L'.K_n/K) \to G(L'/K)) = N_{L'/K}(L'^*),$$

and that

$$\mathrm{Ker}(K^* \to G(L'.K_n)) = N_{L'.K_n/K}((L'.K_{nr})^*),$$

because

$$N_{L'.K_n/K}((L'.K_{nr})^*) = N_{K_n/K}(K_n^*) \cap N_{L'/K}(L'^*),$$

as L'/K is totally ramified and K_n/K is unramified (cf. (2.6.H)).

(11.4.B) DEFINITION OF THE RECIPROCITY ISOMORPHISM.

Choose a uniformizing element π of K. Let $L_\pi = \cup L_m$ be the union of the Lubin-Tate extensions L_n. Then $K^{ab} = K_{nr}.L_\pi$ (11.3.B). Now define

$$\begin{aligned} r: K^* &\longrightarrow G(K^{ab}/K) \\ U(K) \ni u &\longmapsto r(u) = \varphi(u^{-1}) \in G(L_\pi/K) = G(K^{ab}/K_{nr}) \\ \pi &\longmapsto F \in G(K^{ab}/L_\pi) \end{aligned}$$

where F is the Frobenius automorphism of K^{ab}/L_π.

Remarks.

1. This definition checks out with the one given in (11.4.A), because π is a norm from every L_n/K (11.2.G) (cf. (11.4.A.3)).
2. It follows also from (11.4.A.3) that r does not depend on the choice of π in K.
3. Exactly as in the corollary to theorem 3 of [LT] one can prove from remark 2 that r: $K^* \to G(K^{ab}/K)$ is identical with the 'classical' reciprocity isomorphism, given by the norm residue symbol.
   In fact, let s: $K^* \to G(K^{ab}/K)$ be the reciprocity law isomorphism; i.e. $s(a) = (a, K^{ab}/K)$. Let π be any uniformizing element of K. We know that $K^{ab} = K_{nr}.L_\pi$ (11 3.B). The element π is a norm from every $L_n \subset L_\pi$ (11.2.G), hence $s(\pi) := (\pi, K^{ab}/K)$ is the identity on L_π. Furthermore $s(\pi)$ is the Frobenius automorphism on K_{nr}. By the definition of r above (using π and L_π) the same is true for $r(\pi)$. Since the prime elements of K generate K^*, this shows that s = r.
4. The homomorphism r is the restriction to $K^* \subset \tilde{K}^* \simeq U(K) \times \hat{\mathbf{Z}}$ (cf. (11.3.D) Remark 1) of an isomorphism

   $$\tilde{K}^* \simeq U(K) \times \hat{\mathbf{Z}} \xrightarrow{\sim} G(K^{ab}/K)$$

   viz. the isomorphism given by

   $$a = \pi^r u \mapsto (u, r) \mapsto \varphi(u^{-1})F^r$$

   (cf. (11.3.D) Remark 2 and (11.3.C)).

(11.4.C) *Theorem*

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

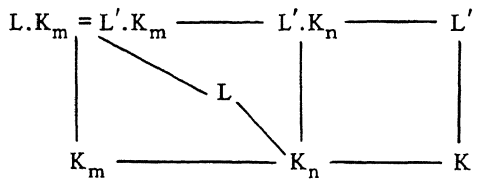
$$\mathrm{Ker}(K^* \to G(K^{ab}/K) \to G(L/K)) = N_{L/K}(L^*).$$

Proof. It suffices to prove that $N_{L/K}(L)$ is contained in this kernel (11.4.A.1). Let K_n be the maximal unramified extension of K contained in L; let r_n: $K_n^* \to G(K_n{}^{ab}/K_n)$ be the analogous homomorphism (for K_n) to r: $K^* \to G(K^{ab}/K)$. Then we have a commutative diagram

(11.4.C.1)

$$\begin{array}{ccc} K_n^* & \xrightarrow{N_{K_n/K}} & K^* \\ \downarrow{\scriptstyle r_n} & & \downarrow \\ G(L/K_n) & \hookrightarrow & G(L/K) \end{array}$$

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, where m is a multiple of the degree $n = [K_n : K]$. Then $K_m \supset K_n$.



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

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

(cf. (11.4.A.3)). It remains to check that

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

Let $u' \in U(\hat{L}'_{nr}) = U(\hat{L}_{nr})$ be any lift of u. The element $u'' := (1+F+\ldots+F^{n-1})(u')$ is then a lift of $N_{K_n/K}(u) = (1+F+\ldots+F^{n-1})(u)$.
The element $r_n(u) \in G(L'.K_m/K_m)$ corresponding to u is, according to (10.2) and (11.4.A), characterized by

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

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

$$\frac{r_n(u)\,(\pi_{L'})}{\pi_{L'}} \equiv \frac{(1+F+\ldots+F^{n-1})\,(u')}{F(1+F+\ldots+F^{n-1})\,(u')} = \frac{u''}{F(u'')} \quad \text{mod. } V(\hat{L}'_{nr})$$

But $r(u) \in G(L'.K_m/K_m)$ is characterized by

$$\frac{r(u)\,(\pi_{L'})}{\pi_{L'}} \equiv \frac{u''}{F(u'')} \quad \text{mod. } V(\hat{L}'_{nr})$$

This shows that $r_n(u) = r(N_{K_n/K}(u))$ for $u \in U(K_n)$. We have shown that the diagram

(11.4.C.2)

$$\begin{array}{ccc} K_n^* & \xrightarrow{N_{K_n/K}} & K^* \\ \downarrow{\scriptstyle r_n} & & \downarrow{\scriptstyle r} \\ G(L'K_m/K_n) & \hookrightarrow & G(L'K_m/K) \end{array}$$

is commutative. It follows that the diagram (11.4.C.2) is also commutative. We know from (11.4.A.2) that the kernel of r_n in diagram (11.4.C.1) is equal to $N_{L/K_n}(L^*)$; it follows that

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

because of the commutativity of (11.4.C.1).

q.e.d.

(11.4.D) *Corollary* (The existence theorem) ([CL] Ch. XIV § 6 Th. 1)

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

(11.4.E) *Corollary*

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

A norm subgroup of K is necessarily open and of finite index (cf. (11.4.A.1)). The other half of Cor. (11.4.D) and (11.4.E) then follow both from the fact that r is the restriction to K^* of some isomorphism

$$\tilde{K}^* \simeq G(K^{ab}/K)$$

(cf. (11.4.C), (11.3.C), (11.3.D) Remark 1 and (11.4.B) Remark 4).

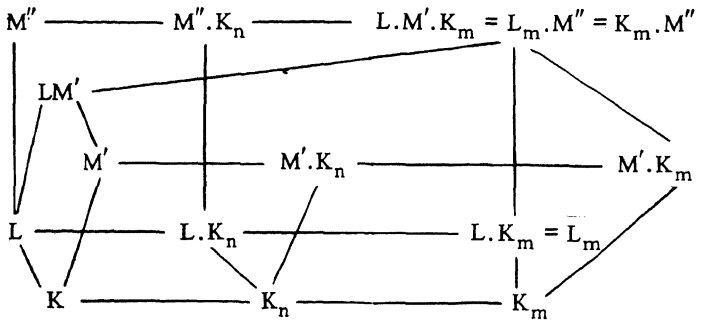
(11.5) **Remarks.**

(11.5.A) A FUNCTORIAL PROPERTY OF THE RECIPROCITY ISOMORPHISM.

The reciprocity homomorphisms $r_K : K^* \to G(K^{ab}/K)$ satisfy a functorial property. In fact if L/K is any finite galois extension of K, then the following diagram is commutative

$$\begin{array}{ccc} L^* & \xrightarrow{N_{L/K}} & K^* \\ \downarrow{\scriptstyle r_L} & & \downarrow{\scriptstyle r_K} \\ G(L^{ab}/L) & \longrightarrow G(K^{ab}.L/L) \hookrightarrow & G(K^{ab}.L/K) \end{array}$$

The commutativity of the diagram (11.4.C.2) proves this for the case that L/K is unramified. It suffices to prove in addition that the diagram above is commutative when L/K is cyclic totally ramified (because G(L/K) is solvable). To this end let M'/K be a totally ramified abelian extension, K_n/K an unramified extension. By means of the same kind of argument as used in (2.8.J) Remark 2 we can find a totally ramified extension M''/K such that $L \subset M''$ and $M''.K_m = M'.L.K_m$ for some unramified extension K_m/K of degree m, where m is a multiple of n, the degree of K_n/K.



Now use M''/L and $L_m = L.K_m$ to define $r_L : L^* \to G(L_m.M''/L)$ and M''/K and K_m/K to define $r_K : K^* \to G(K_m.M''/K)$ (cf. (11.4.A)). It is clear from (10.2) that $r_L(u) = r_K(N_{L/K}(u))$ for $u \in U(L)$. And if π'' is a uniformizing element of M'', we have $r_L(N_{M''/L}(\pi'')) = F \in G(L_m.M''/M'') = G(K_m.M''/M'')$, and if

$\pi_L \in L$ is the uniformizing element $\pi_L := N_{M''/L}(\pi'')$ then $r_K(N_{L/K}(\pi_L)) = r_K(N_{M''/K}(\pi'')) = F \in G(K_m.M''/M'')$.

q.e.d.

(11.5.B) *Problem*

Lubin and Tate show in [LT] that the homomorphism r: $K^* \to G(K^{ab}/K)$ defined by

$$U(K) \ni u \mapsto [u^{-1}]_f \text{ on } L_\pi, \text{ and identity on } K_{nr}$$
$$\pi \mapsto \text{identity on } L_\pi, \text{ and Frobenius on } K_{nr}$$

is independant of the choice of π. It follows that this homomorphism is identical with the homomorphism r (and with the homomorphism defined by the norm residue symbol; cf. (11.4.B) Remark 3). Specifically this means that if $u' \in U(L_m.\hat{K}_{nr})$ is such that

$$\frac{Fu'}{u'} \equiv \frac{[u]_f(\lambda_m)}{\lambda_m} \quad \text{mod. } V(L_m.\hat{K}_{nr})$$

that then $N_{L_m.\hat{K}_{nr}/\hat{K}_{nr}}(u') \in U(K)$ (this follows from (10.1.B)) and

$$N_{L_m.\hat{K}_{nr}/\hat{K}_{nr}}(u') \equiv u \quad \text{mod. } U^m(K).$$

I do not know a direct proof of this fact. (One can use (11.2.A), especially (11.2.A.1), to show that s and r both map $U^m(K)$ into $G(L_\pi/K)^m$ and that the induced maps r,s: $U^m(K)/U^{m+1}(K) \to G(L_\pi/K)^m/G(L_\pi/K)^{m+1}$ are identical.)

REFERENCES.

DG. M. Demazure, P. Gabriel. Groupes Algebriques. North Holland 1969.

LT. J. Lubin, J. Tate. Formal complex multiplication in local fields. Ann. Math. **81** (1965), 380-387.

CAC. J.-P. Serre. Sur les corps locaux à corps residuel algébriquement clos. Bull. Soc. Math. France **89** (1961), 105–154.

CL. J.-P. Serre. Corps locaux. Hermann, 1962.

GP. J.-P. Serre. Groupes pro-algebriques. Publ. Math. de l'I.H.E.S. (1960).

SGAD. Seminaire de Géométrie Algébrique 1963/1964. Schémas en groupes. I.H.E.S.

1. N. Bourbaki. Topologie générale Ch. 1, 2. 3^e ed. Hermann 1961.
2. N. Bourbaki. Algèbre commutative. Ch. 1, 2. Hermann 1961.
3. H. Cartan, S. Eilenberg. Homological algebra. Princeton Univ. Press 1956.
4. B. Dwork. Norm residue symbol in local number fields. Abh. Math. Sem. Hamburg **22** (1958), 180–190.
5. P. Gabriel. Des catégories abéliennes. Bull. Soc. Math. France **90** (1962) 323–448.
6. M.J. Greenberg. Schemata over local fields. Ann. Math. **73** (1961), 624–648.
7. M.J. Greenberg. Algebraic rings. Trans. AMS **111** (1964), 472–481.
8. A. Grothendieck. Sur quelques points d'algèbre homologique. Tohoku Math. J. **9** (1957), 119–221.
9. H. Hasse. Vorlesungen über Klassenkörpertheorie. Physica Verlag, Würzburg 1967.
10. M. Hazewinkel. Corps de classes local. Appendice dans [DG]. (M. Demazure, P. Gabriel Groupes algebriques. North Holland 1969.)
11. N. Jacobson. Lectures in abstract algebra Vol. III. v. Nostrand 1964.
12. S. Lang. Rapport sur la cohomologie des groupes. Benjamin 1966.
13. B. Mitchell. Theory of categories. Acad. Press 1965.
14. F. Oort. Algebraic group schemes in characteristic zero are reduced. Inv. Math. 2 (1966–1967), 79.
15. F. Oort. Embeddings of finite group schemes into abelian schemes. Lecture notes by J. Lubin. Advanced Science Sem. in Algebraic Geometry. Bowdoin College, summer 1967.
16. F. Oort. Commutative group schemes. Lecture notes in math. **15**. Springer 1966.
17. J.-P. Serre. Sur les corps locaux à corps residuel algébriquement clos. Sem. Bourbaki 1958/1959. Exp. 185.

. Serre. Cohomologie galoisienne. Lecture notes in math. 5. Springer, 54.
P. Serre. Local class field theory. Proc. of a conference on algebraic mber theory held in Brighton, ed. by J.W.S. Cassels and A. Fröhlich. ad. Press. 1967, 128–161.
Tate. p-divisible groups. Proc. of a conference on local fields held at Driergen, ed. by T.A. Springer. Springer 1967, 158–183.
Weil. Adèles and algebraic groups. Lecture notes by M. Demazure and Ono. Inst. for Advanced Study, Princeton 1961.
Weiss. Algebraic number theory. McGraw-Hill 1963.

Samenvatting

Zij K een lokaal lichaam, d.w.z. een discreet niet-archimedisch gevalueerd lichaam, dat compleet is in de metriek, die door deze valuatie geïnduceerd wordt.
Veronderstel dat het restklassenlichaam k van K algebraïsch gesloten is. Men kan de groep van eenheden U(K) van K de structuur van een pro-algebraische groep over k geven. Serre bewees in [CAC] dat er bij elke eindige abelse lichaamsuitbreiding L/K een isogenie van U(K) hoort, en dat in zekere zin alle isogenieën van U(K) zo verkregen worden. Hoofdstuk II van dit proefschrift behandelt een generalisatie van deze stelling voor het geval dat k perfect, maar niet noodzakelijk algebraisch gesloten is. Het bewijs sluit nauw aan bij het oorspronkelijke bewijs van Serre.
Veronderstel nu dat het restklassenlichaam k eindig is. Hoofdstuk III begint net als [LT] met de constructie van zekere totaal vertakte abelse uitbreidingen L_m/K. Een stelling over het beeld van de norm-afbeelding $N_{L_m/K}$ stelt ons dan in staat te bewijzen dat de lichaamsuitbreiding $(\cup L_m).K_{nr}$ de maximale abelse uitbreiding van K is (K_{nr} = de maximale onvertakte uitbreiding van K). Met behulp hiervan construeren we een reciprociteits isomorphisme dat identiek blijkt te zijn met het 'klassieke' reciprociteits isomorphisme dat gedefiniëerd wordt door het norm rest symbool.
Het voordeel van deze methode (naar de mening van de schrijver) is dat men de nogal ingewikkelde machinerie kan vermijden die te maken heeft met het bestaan van de zg. fundamentele 2-cocykel (van K).
De mogelijkheid het reciprociteits isomorphisme zo te definieren volgt uit Dwork's beschrijving van dit isomorphisme in [4], en vooral uit de resultaten van Lubin en Tate in [LT]; ze werd trouwens al in 1959 door Serre aangeduid in [17] §7.