The Hebrew University of Jerusalem

The Institute of Mathematics

On Nilpotency Problems in Metabelian Extensions of Local Fields

Sefi Ladkani

December 1996

This work was carried out under the supervision of Prof. Ehud de-Shalit of the Hebrew University of Jerusalem.

I would like to express my deep gratitude to Prof. de-Shalit for his guidance.

Abstract

Let k be a local field. Abelian Local Class Field Theory (LCFT) makes a correspondence between abelian extensions L/k of k and closed subgroups of the completion $\hat{k}^\times$ of the multiplicative group of the field. Lubin and Tate (see [L–T] and [Iw, ch. 4] for an exposition) have constructed a one-dimensional commutative group law, enabling us to define an $\mathfrak{o}_k$-module structure on the maximal ideal of a completion of the algebraic closure of k. The fields generated by torsion points of this module play important role in the development of explicit LCFT.

Recently, De-Shalit and Koch, in [dS–K], developed an analogous theory for metabelian extensions. They introduced the groups $\mathfrak{G}_d(k,\phi)$ and $\mathfrak{G}(k,\phi)$, which in their theory are analogous to the group $\hat{k}^\times$, and defined a correspondence between metabelian extensions of k and closed subgroups of $\mathfrak{G}(k,\phi)$.

This work deals with nilpotency problems concerning metabelian extensions. A nilpotent (finite) group G is characterized by the fact that its lower and upper central series start with G (or 1) and reach 1 (or G).

We bound the center of the group $\mathfrak{G}_d(k,\phi)$ from above and from below. This enables us to show that the group $\mathfrak{G}(k,\phi)$, which correspond to the maximal metabelian of k, is centerless. We also show that the center of a dense subgroup of $\mathfrak{G}_d(k,\phi)$ is isomorphic to $\mathbb{F}_q^\times$. This is done by considering the action of $\hat{k}^\times$ on power series $\mathbb{F}_{q^d}[[X]]^\times$ and showing that the only power series which are fixed by every $u \in U_k$ are the constant series. Another use of this fact is in our proof that the groups $\mathfrak{G}_d(k,\phi)$ cannot be represented as a semi-direct product of $\hat{k}^\times$ and $\mathbb{F}_{q^d}[[X]]^\times$.

Using similar techniques we make some steps toward computing the second element of the upper central series of $\mathfrak{G}_d(k,\phi)$. It follows from our results that this series terminates at a rather small subgroup of $\mathfrak{G}_d(k,\phi)$.

Given a group G, one can search for maximal pro-nilpotent (inverse limit of nilpotent groups) subgroups of G, and also for the maximal pro-nilpotent quotient of G. Given a Galois extension L/K, this correspond to the question of finding maximal pro-nilpotent extensions L/M and the maximal pro-nilpotent extension N/K for $K \subseteq M, N \subseteq L$.

In analogy to Kummer extensions, we construct a family of metabelian extensions which are not nilpotent when the residue field of k is of order $q > 2$. The idea is to add to the fields $k(\omega_n)$, which contain the roots $\pi^{n+1} \cdot \omega_n = 0$, new roots $\pi^{n+1} \cdot \alpha_n = a$ for $a \in k$, and to consider the resulting extensions $k(\omega_n, \alpha_n)/k$, as it is done when adding n-th roots to a field containing the n-th roots of unity.

We deduce that for a non-ramified extension K/k, the metabelian extension $(Kk_\pi^0)^{ab}/K$ is not pro-nilpotent. In the case $q = 2$, the extensions $k(\omega_n, \alpha_n)/k$ are nilpotent, and their nilpotency class can be arbitrarily large.

Finally, we discuss some aspects of the lower central series. We define, for a closed subgroup $H \leq U_k$, subgroups $B_{d,\alpha}(H)$ of $\mathbb{F}_{q^d}[[X]]^\times$, and relate them to nilpotent extensions of L in $(k_d^{nr}k_\pi)^{ab}$, where L is a class field to $P \times H$ for $P \leq \langle \pi^d \rangle^{\hat{\mathbb{Z}}}$. This relation enables us to prove that for a non-ramified extension K/k, the extension $(Kk_\pi)^{ab}/(Kk_\pi^0)$ is pro-nilpotent, and the maximal pro-nilpotent extension of K contained in $(Kk_\pi)^{ab}$ equals the maximal pro-nilpotent extension of $k_{\pi,p}k^{nr}$ contained in $(Kk_\pi)^{ab}$, where $k_{\pi,p}k^{nr}$ is the class field of V, the cyclic subgroup of $(q-1)$-th roots of unity in U_k.

Contents

Part I
Background

1 Local Fields

In this section, we briefly review the basic facts on local fields. For a detailed discussion, including proofs, we refer the reader to [Iw, chapters 1,2].

Basic Definitions

Let k be a field. A *valuation* on k is a function

$$\nu : k^\times \longrightarrow \mathbb{R} \cup \{\infty\}$$

satisfying

$$\begin{aligned} \nu(0) &= +\infty\ ,\ \nu(x) \in \mathbb{R} && \text{for } x \in k^\times \\ \nu(xy) &= \nu(x) + \nu(y) && \forall x, y \in k \\ \nu(x+y) &\geq \min\{\nu(x), \nu(y)\} && \forall x, y \in k \end{aligned}$$

Let

$$\begin{aligned} \mathfrak{o} &= \{x \in k : \nu(x) \geq 0\} \\ \mathfrak{p} &= \{x \in k : \nu(x) > 0\} \end{aligned}$$

$\mathfrak{o}$ is a local ring whose maximal ideal is $\mathfrak{p}$. The field $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ is called the *residue field* of k.

Throughout, we assume that the image $\nu(k^\times)$ is a discrete subgroup of $\mathbb{R}$. In such case we can normalize ν such that $\nu(k^\times) = \mathbb{Z}$.

Let (k, ν) be a field with a normalized valuation. An element $\pi \in k$ for which $\nu(\pi) = 1$ is called a *prime* of k. We have $\mathfrak{p} = \pi\mathfrak{o}$, and every ideal of $\mathfrak{o}$ is of the form $\mathfrak{p}^n = \pi^n\mathfrak{o}$ for $n \geq 1$. Thus $\mathfrak{o}$ is a principal domain.

Let

$$\begin{aligned} U &= \{x \in k : \nu(x) = 0\} \\ U_n &= 1 + \mathfrak{p}^n \end{aligned}$$

$U = \mathfrak{o} \setminus \mathfrak{p}$ is the set of invertible elements of the ring $\mathfrak{o}$, and $k^\times = \langle\pi\rangle \times U$. U_n are multiplicative subgroups of U, and they form a filtration of U. We have

$$U/U_1 \cong \mathfrak{f}^\times$$

canonically, and

$$U_n/U_{n+1} \cong \mathfrak{k}^+$$

non-canonically.

The metric defined by

$$d(x,y) = e^{-\nu(x-y)}$$

equips the groups k^+ and $k^\times$ with the topology it induces. In this topology, the family $\{\mathfrak{p}^n\}$ is a basis of neighborhoods of 0 (which are also subgroups of k^+), and the family $\{U_n\}$ is a basis of neighborhoods of 1 in the group $k^\times$.

A field (k,ν) is *complete* if the metric defined above is complete (i.e. every Cauchy sequence converges). In a complete field, a necessary and sufficient condition for the convergence of an infinite sum (product) is the convergence of the entries in the sum (product) to 0 (1).

Definition. A field (k,ν) is called *local field* if (k,ν) is complete and the residue field $\mathfrak{k}$ is finite.

Let (k,ν) be a local field with residue field $\mathbb{F}_q$. Then U is a compact group. It contains the cyclic group V of the $(q-1)$-th roots of unity. In fact, for every $u \in U$, the limit

$$\lim_{n\to\infty} u^{q^n}$$

exists and equals the root whose image mod $\mathfrak{p}$ equals u mod $\mathfrak{p}$, and we have $U = V \times U_1$.

Ramification

Let k'/k be a finite extension. There is a unique extension of ν to k', denoted by ν'. Denote by $\mathfrak{o}', \mathfrak{p}', \mathfrak{k}'$ the local ring, etc. of k'. The *ramification index* $e(k'/k)$ and *residue degree* $f(k'/k)$ are defined by

$$e(k'/k) = [\nu'(k'^\times) : \nu(k^\times)]$$
$$f(k'/k) = [\mathfrak{k}' : \mathfrak{k}]$$

If $e(k'/k) = 1$, we call the extension k'/k *non-ramified.* If $f(k'/k) = 1$, we call it *totally ramified.* We have the relation

$$[k' : k] = e(k'/k)f(k'/k)$$

An infinite extension K/k is *non-ramified* if every finite extension k'/k contained in K/k is non-ramified. The concept of being totally ramified for such extensions is defined similarly.

For every $d \geq 1$ we have a unique non-ramified extension of degree d over k, denoted by k_d^{nr}. It is Galois over k, and we have

$$\mathrm{Gal}(k_d^{nr}/k) \cong \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}$$

The maximal non-ramified extension over k, denoted by k^{nr}, is the union of the fields k_d^{nr}. Its residue field equals $\bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, and

$$\mathrm{Gal}(k^{nr}/k) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$$

The *Frobenius automorphism* ϕ of k^{nr}/k is the one corresponding to the Frobenius automorphism of $\bar{\mathbb{F}}_q/\mathbb{F}_q$. It is characterized by

$$\phi(x) \equiv x^q \pmod{\mathfrak{p}_{k^{nr}}}$$

and generates (topologically) $\mathrm{Gal}(k^{nr}/k)$.

2 Abelian Local Class Field Theory

As in the previous section, we only define the basic concepts and give the main results, omitting their proofs. For details, we refer the reader to [Iw, ch. 4].

Formal Group Laws

Let R be a commutative ring with 1, and consider the ring of formal power series over R, denoted by $R[[X]]$. Addition and multiplication of power series are defined as usual. We can also define a composition of a power series ξ with a power series $\eta \in XR[[X]]$; if $\xi = \sum_{i=0}^{\infty} a_i X^i$, define

$$\xi \circ \eta = \sum_{i=0}^{\infty} a_i \eta^i$$

and this is well-defined due to our assumption that $\eta \in XR[[X]]$. The composition of power series in more than one variable is defined similarly.

Definition. A *one-dimensional commutative formal group law over R* is a power series $F(X,Y) \in R[[X,Y]]$ satisfying

$$\begin{aligned} F(X,Y) &\equiv X + Y \pmod{\deg 2} \\ F(F(X,Y),Z) &= F(X,F(Y,Z)) \\ F(X,Y) &= F(Y,X) \end{aligned}$$

where by $\pmod{\deg 2}$ we mean that the difference between the expressions in both sides of the equation does not have any terms of degree less than 2 (the degree of a monomial cX^iY^j is $i+j$).

It can be shown that every such a formal group law has the form

$$F(X,Y) = X + Y + \sum_{i,j\geq 1} c_{ij} X^i Y^j$$

We think of F as a group law in the following sense; let $f, g \in XR[[X]]$, then we can define "addition" $\dot{+}$ by

$$f \dot{+} g = F(f(X), g(X))$$

and this definition makes $XR[[X]]$ a commutative group.

A *morphism* f from one group law F to another group law G is a power series $f \in XR[[X]]$ satisfying

$$f(F(X,Y)) = G(f(X), f(Y))$$

If f is invertible (with respect to the composition), it is called an *isomorphism.*

Lubin–Tate Power Series

In [L–T], Lubin and Tate constructed a family of formal group laws. They used such group laws to define an $\mathfrak{o}$-module structure on $\mathfrak{p}_\Omega$ (see below). In this approach to local class field theory, the study of the fields defined by considering the π-torsion points is a crucial step towards the (constructive) definition of the Artin map.

Let (k, ν) be a local field, and let K be the completion of the maximal non-ramified extension k^{nr} of k. Denote by $\mathfrak{o}_K, \mathfrak{p}_K$ the ring of integers of K and its maximal ideal.

Let $\pi \in K$ be a prime element. Denote by $\mathcal{F}_\pi$ the set of power series $h \in \mathfrak{o}_K[[X]]$ for which

$$\begin{aligned} h(X) &\equiv \pi X \pmod{\deg 2} \\ h(X) &\equiv X^q \pmod{\mathfrak{p}_K} \end{aligned}$$

Let ϕ be the extension of the Frobenius automorphism to K. For a power series $F(X,Y) \in \mathfrak{o}_K[[X,Y]]$, denote by $F^\phi(X,Y)$ the power series obtained by applying ϕ on its coefficients.

Let $h \in \mathcal{F}_\pi$. There is a unique formal group law $F_h(X,Y)$ such that

$$h \circ F_h(X,Y) = F_h^\phi(h(X), h(Y))$$

Moreover, for every $a \in \mathfrak{o}$, there is a unique power series $[a]_h \in \mathfrak{o}_K[[X]]$ satisfying

$$\begin{aligned} [a]_h(X) &\equiv aX \pmod{\deg 2} \\ h \circ [a]_h &= [a]_h^\phi \circ h \end{aligned}$$

It follows that $[a]_h$ is an endomorphism of the group law F_h, and the map $a \mapsto [a]_h$ is an injective ring homomorphism:

$$[ab]_h = [a]_h \circ [b]_h$$
$$[a+b]_h = F_h([a]_h(X), [b]_h(X))$$

We note also that if k'/k is a finite non-ramified extension and $\pi \in k'$, $h \in \mathfrak{o}_{k'}[[X]]$, then F_h and all $[a]_h$ have their coefficients in $\mathfrak{o}_{k'}$. In particular, if $\pi \in k$, then $F_h \in \mathfrak{o}[[X,Y]]$ and $[a]_h \in \mathfrak{o}[[X]]$.

If π, π' are two prime elements of K and $h \in \mathcal{F}_h$, $h' \in \mathcal{F}_{h'}$, then there is an isomorphism $\theta \in \mathfrak{o}_K[[X]]$ between the formal groups F_h and F'_h. If, $h, h' \in \mathcal{F}_\pi$ (same π) and $\pi \in k'$, then the isomorphism θ is actually in $\mathfrak{o}_{k'}[[X]]$.

Torsion Points

Let $\pi \in K$, $h \in \mathcal{F}_h$. Fix an algebraic closure Ω of k, and let μ be an extension of ν to Ω. Let $\bar{\Omega}$ be a completion of Ω, with valuation $\bar{\mu}$. As usual, let $\mathfrak{p}_{\bar{\Omega}}$ denote the maximal ideal of $\mathfrak{o}_{\bar{\Omega}}$.

We can define an $\mathfrak{o}$-module structure on $\mathfrak{p}_{\bar{\Omega}}$ by

$$\alpha \dotplus \beta = F_h(\alpha, \beta) \qquad \alpha, \beta \in \mathfrak{p}_{\bar{\Omega}}$$
$$a \cdot \alpha = [a]_h(\alpha) \qquad a \in \mathfrak{o}, \alpha \in \mathfrak{p}_{\bar{\Omega}}$$

Let $n \geq -1$. The π^{n+1}-torsion submodule W_n (we omit the reference to h, but these modules do depend on h) is defined by

$$W_n = \left\{ x \in \mathfrak{p}_{\bar{\Omega}} : \pi^{n+1} \cdot x = 0 \right\}$$

($W_{-1} = 0$). It can be shown that

$$W_n = \left\{ x \in \mathfrak{p}_{\bar{\Omega}} : (\phi^n h \circ \phi^{n-1} h \circ \cdots \circ \phi h \circ h)(x) = 0 \right\}$$

and that these modules are finite, $|W_n| = q^{n+1}$.

Let $\widetilde{W}_n = W_n \setminus W_{n-1}$. Any element $\omega_n \in \widetilde{W}_n$ generates W_n as an $\mathfrak{o}$-module, that is, $W_n = \mathfrak{o} \cdot \omega_n$, and there is an isomorphism $W_n \cong \mathfrak{o}/\mathfrak{p}^{n+1}$ defined by $a \mapsto a \cdot \omega_n$ (non-canonically).

The group of module automorphisms of W_n is denoted by $\operatorname{Aut} W_n$. Every $u \in U$ defines an automorphism $\omega \mapsto u \cdot \omega$. In fact, the automorphisms defined in this way are all possible automorphisms, and we have an isomorphism of groups

$$U/U_{n+1} \cong \operatorname{Aut} W_n \tag{2.1}$$

induced by mapping u into the automorphism it defines.

The fields $k^{nr}(W_n)$ do not depend on the particular choice of π and $h \in \mathcal{F}_\pi$.

Let k'/k be non-ramified. If $\pi \in k'$, $h \in \mathcal{F}_\pi \cap \mathfrak{o}_{k'}[[X]]$, then the fields $k'(W_n)$ do not depend on h. The extensions $k'(W_n)/k'$ are Galois, totally ramified of degree $(q-1)q^n$. If ω_n is a generator of W_n, then $k'(W_n) = k'(\omega_n)$ and ω_n is a prime in that extension.

The homomorphism

$$\mathrm{Gal}(k'(W_n)/k') \longrightarrow \mathrm{Aut}\, W_n$$

defined by restricting $\sigma \in \mathrm{Gal}(k'(W_n)/k')$ to W_n is an isomorphism. Combining this and (2.1) we get that

$$\mathrm{Gal}(k'(W_n)/k') \cong U/U_{n+1} \tag{2.2}$$

Consider now the module $W_\infty = \bigcup_{n=-1}^{\infty} W_n$ and the field $k'(W_\infty)$ (which is the union of the fields $k'(W_n)$). It is clear that

$$W_\infty = \left\{ x \in \mathfrak{p}_{\bar{\Omega}} : \text{ there is an } n \geq -1 \text{ for which } \pi^{n+1} \cdot x = 0 \right\}$$

The following diagram, consisting of the isomorphisms in (2.2), is commutative, for $m \geq n$;

$$\begin{array}{ccc} \mathrm{Gal}(k'(W_m)/k') & \xrightarrow{\cong} & U/U_{m+1} \\ {\scriptstyle res}\downarrow & & \downarrow \\ \mathrm{Gal}(k'(W_n)/k') & \xrightarrow{\cong} & U/U_{n+1} \end{array}$$

where the left vertical arrow is the restriction map, and the right vertical arrow is the canonical map. Therefore, we get an isomorphism

$$\mathrm{Gal}(k'(W_\infty)/k') = \varprojlim_n \mathrm{Gal}(k'(W_n)/k') \cong \varprojlim_n U/U_{n+1} = U$$

One can verify that the explicit form of this homomorphism, denoted by $\delta : U \to \mathrm{Gal}(k'(W_\infty)/k')$, is given by

$$\delta(u)(\omega) = u \cdot \omega$$

for every torsion point $\omega \in W_\infty$.

Main Results of Abelian Local Class Field Theory

Let $\pi \in k$, $h \in \mathcal{F}_\pi \cap \mathfrak{o}[[X]]$. Denote by k_π the field $k(W_\infty)$ (which does not depend on h), and let $L_k = k^{nr} k_\pi$.

The extension L_k/k is abelian, and the Frobenius automorphism ϕ of k^{nr}/k can be uniquely extended to an automorphism ψ_π of L_k, whose fixed field contains k_π.

Definition. The *Artin map* $\rho_k : \hat{k}^\times \to \mathrm{Gal}(L_k/k)$ is defined by

$$\rho_k(a) = \psi_\pi^\nu \delta(u^{-1})$$

for $a = \pi^\nu u$, $\nu \in \hat{\mathbb{Z}}$, $u \in U$.

One can show that this definition of ρ_k does not depend on the particular choice of $\pi \in k$.

Definition. Let F/k be an extension. The *norm group* $N(F/k)$ is

$$N(F/k) = \bigcap_{\substack{k \subset k' \subset F \\ [k':k] < \infty}} N_{k'/k}(\widehat{k'}^\times)$$

where $N_{k'/k}$ is the usual norm from $k'^\times$ to $k^\times$ (extended to the completions).

Theorem. *Let k be a local field. Denote by k^{ab} the maximal abelian extension over k. Then:*

1. *For every prime $\pi \in k$,*

$$k^{ab} = k^{nr} k_\pi$$

2. *The correspondence*

$$F/k \longmapsto N(F/k)$$

is one-to-one and onto from the set of abelian extensions F/k to the set of closed subgroups of $\hat{k}^\times$. If k'/k is abelian and finite, then

$$[k' : k] = [\hat{k}^\times : N(k'/k)]$$

(the first equality of LCFT).

3. *For every abelian extension F/k, we have*

$$\rho_k(N(F/k)) = \mathrm{Gal}(k^{ab}/F)$$

and this induces an isomorphism

$$\hat{k}^\times / N(F/k) \cong \mathrm{Gal}(F/k)$$

For a proof, we refer the reader to [Iw, ch. 6].

3 Coleman's Norm Operator

Fix a non-ramified extension k'/k, with residue field $\mathfrak{f}'$. Let $\pi \in k$, $h \in \mathcal{F}_\pi \cap \mathfrak{o}_k[[X]]$. For $\alpha \in \mathfrak{p}_{\bar{\Omega}}$, and $g \in \mathfrak{o}_{k'}((X))$, define

$$g(X \dot{+} \alpha) = g \circ F_h(X, \alpha)$$

Coleman defined in [Co] the *norm operator*

$$\mathcal{N}_h : \mathfrak{o}_{k'}((X))^\times \longrightarrow \mathfrak{o}_{k'}((X))^\times$$

by

$$\mathcal{N}_h(g) \circ h = \prod_{\omega \in W_0} g(X \dot{+} \omega)$$

This operator is well defined, and satisfies the following properties:

$$\begin{aligned} \mathcal{N}_h(g_1 g_2) &= \mathcal{N}_h(g_1)\mathcal{N}_h(g_2) \\ \mathcal{N}_h(g) &\equiv g^\phi \pmod{\mathfrak{p}_{k'}} \\ \mathcal{N}_h(g) &\equiv 1 \pmod{\mathfrak{p}_{k'}^{i+1}} \qquad \text{if } g \equiv 1 \pmod{\mathfrak{p}_{k'}^{i}} \end{aligned}$$

One can define the n-th iteration of $\mathcal{N}_h$, by induction:

$$\mathcal{N}_h^{n+1}(g) = \mathcal{N}_h(\mathcal{N}_h^n(g))$$

We have that

$$\mathcal{N}_h^{n+1}(g) \equiv \phi \mathcal{N}_h^n(g) \pmod{\mathfrak{p}_{k'}^{n+1}}$$

thus the limit

$$\mathcal{N}_h^\infty(g) = \lim_{n\to\infty} \phi^{-n} \mathcal{N}_h^n(g)$$

exists and satisfies

$$\mathcal{N}_h(\mathcal{N}_h^\infty(g)) = \phi \mathcal{N}_h^\infty(g)$$

Definition. A power series $g \in \mathfrak{o}_{k'}((X))^\times$ which satisfies

$$\mathcal{N}_h(g) = \phi g$$

is called a *Coleman power series.*

The set of all Coleman power series is a subgroup of $\mathfrak{o}_{k'}((X))^\times$ which will be denoted by $\mathcal{C}(k', h)$.

Lemma 3.1. *Let $g \in \mathcal{C}(k', h)$, $u \in U$. Then*

$$g \circ [u]_h \in \mathcal{C}(k', h)$$

Proof. Since u acts as a permutation on W_0, and $[u]$ commutes with F_h, we have

$$\mathcal{N}_h(g \circ [u]) \circ h = \prod_{\omega \in W_0} g \circ [u] \circ F_h(X, \omega) = \prod_{\omega \in W_0} g \circ F_h([u](X), u \cdot \omega) =$$
$$\prod_{\omega \in W_0} g \circ F_h(X, \omega) \circ [u] = \mathcal{N}_h(g) \circ h \circ [u] = \mathcal{N}_h(g) \circ [u]^{\phi} \circ h$$

hence

$$\mathcal{N}_h(g \circ [u]) = \mathcal{N}_h(g) \circ [u]^{\phi}$$

and the lemma follows. □

Theorem. *There is a split short exact sequence*

$$1 \longrightarrow 1 + \pi \mathfrak{o}_{k'}[[X]] \longrightarrow \mathfrak{o}_{k'}((X))^{\times} \xrightarrow{\mathcal{N}_h^{\infty}} \mathcal{C}(k', h) \longrightarrow 1$$

The splitting $i : \mathcal{C}(k', h) \longrightarrow \mathfrak{o}_{k'}((X))^{\times}$ *is the identity homomorphism.*

For the proof, see [Co].

Corollary. *Reduction modulo* $\mathfrak{p}_{k'}$ *is an isomorphism*

$$\mathcal{C}(k', h) \cong \mathfrak{f}'((X))^{\times}$$

Thus for any $\xi \in \mathfrak{f}'((X))^{\times}$ *there is a unique lifting to Coleman power series* $g_\xi \in \mathcal{C}(k', h)$ *such that*

$$g_\xi \bmod \mathfrak{p}_{k'} = \xi$$

Normed sequences

For $n \geq 0$, denote by k'_n the field $k'(W_n)$.

Definition. A sequence $(\beta_n)_{n \geq 0}$, $\beta_n \in k'_n$ is called *normic* if, for every $m \geq n$,

$$N_{k'_m/k'_n}(\beta_m) = \beta_n$$

Due to the transitivity of the norm, it is sufficient to take $m = n + 1$ in the above definition.

Let $(\omega_n)_{n \geq 0}$ be a sequence such that

$$\pi \cdot \omega_0 = 0$$
$$\pi \cdot \omega_{n+1} = \omega_n \qquad \text{for every } n \geq 0$$

Then for every $n \geq 0$, ω_n is a generator of the module W_n.

Lemma 3.2. *Let $g \in \mathcal{C}(k', h)$, and let, for every $n \geq 0$,*

$$\beta_n = g^{\phi^{-n}}(\omega_n)$$

Then $(\beta_n)_{n\geq 0}$ is normic.

Proof. This is a straightforward computation:

$$\begin{aligned} N_{k'_{n+1}/k'_n}(\beta_{n+1}) &= \prod_{\sigma \in \mathrm{Gal}(k'_{n+1}/k'_n)} \sigma(g^{\phi^{-(n+1)}}(\omega_{n+1})) \\ &= \prod_{u \in U_n/U_{n+1}} g^{\phi^{-(n+1)}}(u \cdot \omega_{n+1}) \\ &= \prod_{\omega \in W_0} g^{\phi^{-(n+1)}}(\omega_{n+1} \dot{+} \omega) \\ &= \mathcal{N}_h(g^{\phi^{-(n+1)}}) \circ h(\omega_{n+1}) = g^{\phi^{-n}} \circ \omega_n = \beta_n \end{aligned}$$

□

This converse of this lemma is also true (although it is much harder to prove), see [Co]. We thus have

Theorem. *There is a one-to-one and onto correspondence between Coleman power series and normic sequences, given by*

$$g \longmapsto (g^{\phi^{-n}}(\omega_n))_{n\geq 0}$$

Definition. A power series $h \in \mathcal{F}_\pi$ is called *normic* if

$$X \in \mathcal{C}(k', h)$$

It follows that for a normic power series, the sequence $(\omega_n)_{n\geq 0}$ is normic (since it corresponds to X).

4 Power Series over Fields

The rings of power series $\mathbb{F}_{q^d}[[X]]$ and $\bar{\mathbb{F}}_q[[X]]$ play a major role in the sequel. To provide a better understanding of these rings, the basic facts concerning power series over fields are presented in this section.

Let F be a field, and $F((X))$ be the field of formal Laurent series over F, that is, the set

$$\left\{ \xi = \sum_{i=-n}^{\infty} a_i X^i \ : \ n \in \mathbb{Z}, a_i \in F \right\}$$

where addition and multiplication are defined in the ordinary way.

Define a valuation v on $F((X))$ by

$$v(\sum_{i=-n}^{\infty} a_i X^i) = \min\{i \in \mathbb{Z} : a_i \neq 0\}\,.$$

This valuation induces a complete metric on $F((X))$. The ring $F[[X]]$ of formal power series over F is exactly the ring of Laurent series with non-negative valuation, and the group of units equals the multiplicative group $F[[X]]^\times$ of invertible power series.

It follows that a basis of open neighborhoods of 1 in $F[[X]]^\times$ is given by the family of subgroups $\{1 + X^n F[[X]]\}$.

Composition

The composition of power series over F is defined exactly as in the case of a general commutative ring R. We have the associative law

$$\xi \circ (\eta \circ \zeta) = (\xi \circ \eta) \circ \zeta$$

for any $\xi \in F[[X]]$ and $\eta, \zeta \in XF[[X]]$, and also the distributive laws

$$\begin{aligned}(\xi_1 + \xi_2) \circ \eta &= \xi_1 \circ \eta + \xi_2 \circ \eta \\ (\xi_1 \xi_2) \circ \eta &= (\xi_1 \circ \eta)(\xi_2 \circ \eta)\end{aligned}$$

Composition is a continuous operation, as the following lemma indicates.

Lemma 4.1. *Let $\xi_n \to \xi$ be a convergent sequence of power series and $\eta_n \to \eta$ be a convergent sequence of power series having no constant term. Then*

$$\xi_n \circ \eta_n \longrightarrow \xi \circ \eta$$

Proof. Write

$$\begin{aligned}\xi \circ \eta - \xi_n \circ \eta_n &= \xi \circ \eta - \xi \circ \eta_n + \xi \circ \eta_n - \xi_n \circ \eta_n \\ &= \xi \circ \eta - \xi \circ \eta_n + (\xi - \xi_n) \circ \eta_n\end{aligned} \tag{4.1}$$

Let $m \geq 0$. Since $\xi_n \to \xi$, we have N_1 such that $v(\xi - \xi_n) \geq m$ for every $n > N_1$. The power series η_n have no constant terms, hence

$$v((\xi - \xi_n) \circ \eta_n) \geq m \tag{4.2}$$

for every $n > N_1$.

Now, write $\xi = \sum_{i=0}^{\infty} a_i X^i$. It follows that

$$\xi \circ \eta - \xi \circ \eta_n = \sum_{i=1}^{\infty} a_i (\eta^i - \eta_n^i) \tag{4.3}$$

(the constant terms a_0 cancel each other). Since $\eta_n \to \eta$, we have N_2 such that $v(\eta - \eta_n) \geq m$ for every $n > N_2$. From

$$\eta^i - \eta_n^i = (\eta - \eta_n) \sum_{j=0}^{i-1} \eta^{i-1-j} \eta_n^j$$

and (4.3), we get that for every $n > N_2$,

$$v(\xi \circ \eta - \xi \circ \eta_n) \geq m$$

Combining this with (4.1) and (4.2), we conclude that for $n > \max\{N_1, N_2\}$,

$$v(\xi \circ \eta - \xi_n \circ \eta_n) \geq m$$

□

Raising to p^n-th powers

Assume now that $\operatorname{char} F = p$.

Lemma 4.2. *The mapping $\xi \mapsto \xi^p$ is a continuous ring homomorphism of $F[[X]]$.*

Proof. We start by proving that this mapping is a ring homomorphism. It is clear that $(\xi\eta)^p = \xi^p \eta^p$. Moreover, we have

$$(\xi + \eta)^p = \xi^p + \eta^p + \sum_{i=1}^{p-1} \binom{p}{i} \xi^i \eta^{p-i}$$

Since $\binom{p}{i}$ are divisible by p for $1 \leq i \leq p-1$ and $\operatorname{char} F = p$, the sum in the RHS of the equation is 0, hence $(\xi + \eta)^p = \xi^p + \eta^p$ and $\xi \mapsto \xi^p$ is indeed a ring homomorphism.

Regarding continuity, it suffices to show that if $\xi_n \to 0$, then $\xi_n^p \to 0$. But this is clear, as $v(\xi_n) \geq m$ yields $v(\xi_n^p) \geq pm$. □

Lemma 4.3. *let $\xi \in 1 + XF[[X]]$. Then* $\lim_{n\to\infty} \xi^{p^n} = 1$.

Proof. We prove by induction on $n \geq 0$, that

$$\xi^{p^n} \in 1 + X^{p^n} F[[X]] \quad .$$

This is clear for $n = 0$. Write $\xi^{p^n} = 1 + X^{p^n} \xi'$. Then

$$\xi^{p^{n+1}} = (\xi^{p^n})^p = (1 + X^{p^n} \xi')^p = 1 + X^{p^{n+1}} \xi'^p$$

and the assertion follows.

Since $\{1 + X^m F[[X]]\}$ is a basis of neighborhoods of 1, it follows that $\lim_{n\to\infty} \xi^{p^n}$ exists and equal to 1. □

If F is also a finite field, we can say even more.

Lemma 4.4. *Assume also that F is finite, and let $\xi \in F[[X]]^\times$. Then*

$$\lim_{n\to\infty} \xi^{(|F|-1)p^n} = 1$$

Proof. Since F is finite, the multiplicative group $F^\times$ is cyclic of order $|F|-1$. Thus $a^{|F|-1} = 1$ for every $a \in F^\times$.

Write ξ as $a_0 + X\xi_1$. The constant term of $\xi^{|F|-1}$ is $a_0^{|F|-1} = 1$, so that $\xi^{|F|-1} \in 1 + XF[[X]]$. Now the result follows from the previous lemma. ☐

Endomorphisms of $F[[X]]^\times$

We state and prove a criterion for the surjectivity of certain endomorphisms of $F[[X]]^\times$. To make the exposition as general as possible, we have chosen to use the language of group rings.

Let $G = \operatorname{Aut} F$, and let $\mathbb{Z}[G]$ be its group ring over $\mathbb{Z}$. Let $\chi = \sum_{\psi\in G} c_\psi \psi$ be an element of $\mathbb{Z}[G]$, such that $c_\psi = 0$ for every $\psi \in G$ except for a finite number of ψ-s.

χ gives rise to the endomorphisms of the multiplicative and the additive groups of F, respectively:

$$\chi^\times : F^\times \to F^\times$$
$$\chi^+ : F^+ \to F^+$$

defined by

$$\chi^\times(x) = \prod_{\psi\in G} \psi(x)^{c_\psi}$$
$$\chi^+(x) = \sum_{\psi\in G} c_\psi \psi(x)$$

where multiplication of $y \in F$ by $c \in \mathbb{Z}$ is understood as a shorthand for writing $y + y + \cdots + y$ where the addition is done c times.

Since there is only finite number of $c_\psi \neq 0$, the above endomorphisms are indeed well-defined.

In addition to these endomorphisms, χ gives rise to an endomorphism of the multiplicative group of $F[[X]]$ as described below.

Let $\xi \in F^\times$ be an invertible power series. Write

$$\xi = \sum_{i=0}^{\infty} a_i X^i$$

For $\psi \in G$, define $\psi(\xi)$ as the power series obtained from ξ by applying ψ on the coefficients:

$$\psi(\xi) = \sum_{i=0}^{\infty} \psi(a_i) X^i \tag{4.4}$$

For general $\chi = \sum_{\psi \in G} c_\psi \psi$, define

$$\chi^{\square} : F^\times \longrightarrow F^\times$$

by

$$\chi^{\square}(\xi) = \prod_{\psi \in G} \psi(\xi)^{c_\psi}$$

where $\psi(\xi)$ is defined in (4.4). Again, $\chi^{\square}$ is well-defined as all but a finite number of the elements in the product are equal to 1.

Proposition 4.5. *Let $\chi \in \mathbb{Z}[G]$ be as above, and suppose that both $\chi^\times$ and χ^+ are surjective endomorphisms.*

Then the endomorphism $\chi^{\square}$ is also surjective.

Proof. Write $U = F[[X]]^\times$, $U_n = 1 + X^n F[[X]]$. Since U_n are subgroups which are invariant under coefficient-wise endomorphisms, we have $\chi^{\square}(U_n) \subseteq U_n$ (recall that $\chi^{\square}$ is a product of the coefficient-wise automorphisms ψ).

From the formulae

$$\prod_\psi \psi(a_0 + \dots)^{c_\psi} = (\prod_\psi \psi(a_0)^{c_\psi}) + \dots$$
$$\prod_\psi \psi(1 + a_n X^n + \dots)^{c_\psi} = 1 + (\sum_\psi c_\psi \psi(a_n)) X^n + \dots$$

we get that the following diagrams commute:

$$\begin{tikzcd} U \arrow[r, "\chi^{\square}"] \arrow[d, "p_0"'] & U \arrow[d, "p_0"] \\ U/U_1 \arrow[r, "\chi^\times"] & U/U_1 \end{tikzcd} \tag{4.5}$$

$$\begin{tikzcd} U_n \arrow[r, "\chi^{\square}"] \arrow[d, "p_n"'] & U_n \arrow[d, "p_n"] \\ U_n/U_{n+1} \arrow[r, "\chi^+"] & U_n/U_{n+1} \end{tikzcd} \tag{4.6}$$

where the vertical mappings p_n are defined by

$$\begin{aligned} p_0(a_0 + a_1 X + \dots) &= a_0 \\ p_n(1 + a_n X^n + \dots) &= a_n \qquad , \qquad n \geq 0 \end{aligned}$$

and the quotients U/U_1, U_n/U_{n+1} are identified with $F^\times$, F^+.

Let $\eta \in U$. By (4.5) and the assumption that $\chi^{\times}$ is surjective, we can find $\xi_1 \in U$ such that

$$\eta_1 = \frac{\eta}{\chi^{\square}(\xi_1)} \in U_1$$

Assume that we have been able to find $\xi_1, \ldots, \xi_n$ such that

$$\eta_n = \frac{\eta}{\chi^{\square}(\xi_1 \cdot \cdots \cdot \xi_n)} \in U_n \tag{4.7}$$

Then, by (4.6) and the assumption that χ^{+} is surjective, we can find $\xi_{n+1} \in U_n$ such that

$$\eta_{n+1} = \frac{\eta_n}{\chi^{\square}(\xi_{n+1})} \in U_{n+1}$$

Consider now the product $\prod_{n=1}^{\infty} \xi_n$. As $\xi_{n+1} \in U_n$, this product converges to $\xi \in U$. Moreover, by (4.7) it follows that $\eta = \chi^{\square}(\xi)$. As η was arbitrary, we deduce that $\chi^{\square}$ is surjective. $\square$

In the following proposition, we list two corollaries of proposition 4.5 which will be important in the sequel.

Proposition 4.6. *Let ϕ be the Frobenius automorphism of $\bar{\mathbb{F}}_q$, and let $d, e \geq 1$. Then the following endomorphisms of $\bar{\mathbb{F}}_q[[X]]^{\times}$ are surjective:*

$$\xi \longmapsto \frac{\phi^d \xi}{\xi} \tag{4.8}$$

$$\xi \longmapsto \prod_{i=0}^{e-1} \phi^{i \cdot d} \xi \tag{4.9}$$

Proof. These mappings correspond to the elements $A = \phi^d - 1$ and $B = 1 + \phi^d + \cdots + \phi^{(e-1)d}$ in the group ring $\mathbb{Z}[\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)]$. By the last proposition, it is sufficient to check the surjectivity of the endomorphisms defined by these elements on $\bar{\mathbb{F}}_q^{\times}$ and $\bar{\mathbb{F}}_q^{+}$.

For every $x \in \bar{\mathbb{F}}_q$, $\phi(x) = x^q$. Therefore, A and B induce on $\bar{\mathbb{F}}_q^{\times}$ the mappings

$$x \mapsto x^{q^d - 1}$$
$$x \mapsto x^{1 + q^d + \cdots + q^{(e-1)d}}$$

whose surjectivity follows from the fact that $\bar{\mathbb{F}}_q$ is algebraically closed.

Similarly, the mappings on $\bar{\mathbb{F}}_q^{+}$ induced by A and B are

$$x \mapsto x^{q^d} - x$$
$$x \mapsto x + x^{q^d} + \cdots + x^{q^{(e-1)d}}$$

Again, these mappings are surjective since $\bar{\mathbb{F}}_q$ is algebraically closed. $\square$

5 The Groups $\mathfrak{G}_d(k,\phi)$

In this section we define, for every $d \geq 1$, the groups $\mathfrak{G}_d(k,\phi)$, and prove some of their basic properties. These groups were introduced in [dS–K] to describe the Galois groups $\mathrm{Gal}((k_d^{nr}k_\pi)^{ab}/k)$. Their role in the theory of metabelian extensions is analogous to the role of the group $\hat{k}^\times$ in the abelian theory.

We prove here new result about the action of U on power series in $\mathbb{F}_{q^d}((X))$ through composition with $\{u\}$. This result will be used in the computation of the upper central series of the groups $\mathfrak{G}_d(k,\phi)$. A nice application of this result, on the H^2 class corresponding to the extension $\mathfrak{G}_d(k,\phi)$ of $\mathbb{F}_{q^d}[[X]]^\times$ by $\hat{k}^\times$, is given here. Namely, we show that this class is not trivial.

Setup

Let (k,ν) be a local field, with $\mathfrak{o}$ its ring of integers, $\mathfrak{p}$ the maximal ideal in $\mathfrak{o}$, and $\mathbb{F}_q$ the residue field. Let U denote the group of units in $\mathfrak{o}$.

Let ϕ be the Frobenius automorphism on k^{nr}/k, and fix once and for all an extension of ϕ to the separable closure of k, k^{sep}/k. Call this extension also ϕ. The fixed field of ϕ in k^{ab} is a maximal totally ramified abelian extension, hence it equals k_π for some prime $\pi \in k$.

Let $h(X) \in \mathcal{F}_\pi$ be a normic Lubin-Tate power series. As before, we have the formal group law $F_h(X,Y) \in \mathfrak{o}[[X,Y]]$ which satisfies

$$h \circ F_h(X,Y) = F_h^\phi(h(X), h(Y)$$

and have the automorphisms $[a]_h \in \mathfrak{o}[[X]]$ for which

$$[a]_h(X) \equiv aX \pmod{\deg 2}$$
$$h \circ [a]_h = [a]_h \circ h$$

In the sequel, we omit the subscript h, meaning that h has been fixed once and for all.

For each $a \in \mathfrak{o}$, we define $\{a\}$ to be the reduction of $[a]$ modulo $\mathfrak{p}$. Since $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_q$, we certainly have $\{a\} \in \mathbb{F}_q[[X]]$. By $[\pi] = h \equiv X^q \pmod{\mathfrak{p}}$, we get that $\{\pi\} = X^q$.

Lemma 5.1. *If $u \in U_n$, then $\{u\} \equiv X \pmod{deg\ q^n}$.*

Proof. Write $u = 1 + a\pi^n$ for $a \in \mathfrak{o}$. Then

$$[u] = F_h(X,[a\pi^n]) = X + [a\pi^n] + \sum_{i,j\geq 1} c_{ij}X^i[a\pi^n]^j$$

Reducing modulo $\mathfrak{p}$, and using $\{\pi^n\} = X^{q^n}$, we get that

$$\{u\} = X + \{a\}(X^{q^n}) + \sum_{i,j\geq 1} c_{ij}X^i(\{a\}(X^{q^n}))^j$$

As $\{a\}$ is divisible by X, $\{a\}(X^{q^n})$ is divisible by X^{q^n}. We therefore see that the right sum is divisible by X^{q^n+1}, hence

$$\{u\} \equiv X + \bar{a}X^{q^n} \pmod{\deg q^n + 1}$$

($\bar{a} = a \bmod \mathfrak{p}$) and the lemma follows. $\square$

Remark. The proof of the lemma shows also that if $u \notin U_{n+1}$, then

$$\{u\} \not\equiv X \pmod{\deg q^n + 1} \quad .$$

Lemma 5.2. *The mapping* $U \longrightarrow (\mathbb{F}_q[[X]], \circ)$ *defined by*

$$u \longmapsto \{u\}$$

is a continuous injection.

Proof. We already know that $\{uv\} = \{u\} \circ \{v\}$ for $u, v \in U$. To prove that the mapping is an injection, take $u \neq 1$. Then $u \notin U_{n+1}$ for some $n \geq 0$, and by the above remark,

$$\{u\} \not\equiv X \pmod{\deg q^n + 1}$$

therefore $\{u\} \neq X$.

The continuity of this map follows directly from the last lemma, which ensures that elements in smaller neighborhoods of 1 are mapped to power series in smaller neighborhoods of 1. $\square$

Definition of $\mathfrak{G}_d(k, \phi)$

Let $\hat{k}^\times$ be the completion of $k^\times$ defined by

$$\hat{k}^\times = \langle \pi \rangle^{\hat{\mathbb{Z}}} \times U$$

(π is a fixed prime element of k). The group $\hat{k}^\times$ acts on the group of power series $\bar{\mathbb{F}}_q[[X]]^\times$ by

$$\xi^a = \phi^{-\nu} \xi \circ \{u\} \tag{5.1}$$

where $a = \pi^\nu u$, $\nu \in \hat{\mathbb{Z}}$, $u \in U$.

Let $b = \pi^\mu v$. Then

$$\begin{aligned}(\xi^a)^b &= \phi^{-\mu}(\phi^{-\nu}\xi \circ \{u\}) \circ \{v\} = \phi^{-\mu-\nu}\xi \circ \{u\} \circ \{v\} = \\ &= \phi^{-(\mu+\nu)}\xi \circ \{u \cdot v\} = \xi^{ab}\end{aligned}$$

so that (5.1) is indeed a group action.

The following proposition shows that there are not too many power series which are fixed by U.

Proposition 5.3. *Let $\xi \in \mathbb{F}_{q^d}((X))$, and let $H \leq U$ be a subgroup of finite index. Assume that for every $u \in H$,*

$$\xi \circ \{u\} = \xi$$

Then ξ is a constant series.

Proof. Denote by k' the field k_d^{nr}. Let $g_\xi \in \mathcal{C}(k', h)$ be the lifting of g to a Coleman power series. Then by lemma 3.1, $g_\xi \circ [u]$ is also a Coleman power series, and from

$$g_\xi \circ [u] \equiv \xi \circ \{u\} \pmod{\mathfrak{p}_{k'}}$$

we deduce that it is the lifting of $\xi \circ \{u\}$ to $\mathcal{C}(k', h)$. As $\xi = \xi \circ \{u\}$ for every $u \in H$, and the lifting is unique, we get that

$$g_\xi \circ [u] = g_\xi$$

for every $u \in H$.

Define a sequence of generators (ω_n) by

$$\pi \cdot \omega_0 = 0$$
$$\pi \cdot \omega_{n+1} = \omega_n$$

By the correspondence between Coleman power series and norm-compatible sequences, we get that the sequence (β_n) defined by

$$\beta_n = {g_\xi}^{\phi^{-n}}(\omega_n)$$

is normic. From now on, we consider the subsequence (γ_n) obtained from (β_n) by taking the values appearing at places which are integral multiples of d. We have

$$\gamma_n = {g_\xi}^{\phi^{-dn}}(\omega_{dn}) = g_\xi(\omega_{dn})$$

(recall that $g_\xi \in \mathfrak{o}_{k'}[[X]]$ on which ϕ^d acts trivially), and

$$(g_\xi \circ [u])(\omega_{dn}) = g_\xi([u]\omega_{dn}) = g_\xi(\delta(u)(\omega_{dn})) = \delta(u)(g_\xi(\omega_{dn})) = \delta(u)(\gamma_n) \tag{5.2}$$

where δ is the isomorphism between U and $\mathrm{Gal}(k'(W_\infty)/k')$.

Since H as a finite index in U, there is $N \geq 1$ such that $U_{d(N+1)} \leq H$. Let $L = k'(W_{dN})$. By (5.2) we get that

$$\sigma(\gamma_n) = \gamma_n$$

for every automorphism $\sigma \in \mathrm{Gal}(k'(W_\infty)/L)$, thus $\gamma_n \in L$ for every $n \geq N$.

Let $n \geq N$. Since $\gamma_{n+1} \in L$ and $[k'(W_{d(n+1)}) : k'(W_{dn})] = q^d$, we get that

$$\gamma_n = N_{k'(W_{d(n+1)})/k'(W_{dn})}(\gamma_{n+1}) = \gamma_{n+1}^{q^d}$$

thus

$$\gamma_n = \gamma_{n+m}^{q^{dm}} \tag{5.3}$$

for every $m \geq 0$.

The residue field of L is of order q^d (L is a totally ramified extension of k_d^{nr}). Therefore, for every $x \in \mathfrak{o}_L$, the sequence $(x^{q^{dm}})_{m\geq 0}$ converges to a $(q^d - 1)$-th root of unity (or to zero). By (5.3) we deduce that γ_n, for every $n \geq N$, is a root of unity (or 0). Therefore $\gamma_n \in k'$ and

$$\gamma_n = v \in V_{q^d-1} \cup \{0\}$$

for *every* $n \geq 0$. It follows that $\beta_n \in k'$ and $\beta_n = v^{q^{n \bmod d}}$

The power series corresponding to such normic sequences are exactly the constant series. Hence g_ξ is a constant series, thus $\xi \in \mathbb{F}_{q^d}^\times$. □

Definition. Let A, B be commutative groups, and assume that there is an action of A on B, that is, there is a homomorphism $\psi : A \to \operatorname{Aut} B$. Denote by b^a the action of $a \in A$ on $b \in B$.

Define the semi-direct product $A \ltimes B$ by

$$A \ltimes B = \Big\{(a, b) : a \in A, b \in B\Big\} \tag{5.4}$$

where multiplication of (a, b) and (a', b') is defined as

$$(a, b)(a', b') = (aa', b + b'^a) \tag{5.5}$$

(we use multiplicative notation for A, and additive notation for B).

It is easy to verify that this definition satisfies the associative law, the identity is $(1, 0)$, and the inverse of (a, b) is $(a^{-1}, -b^{a^{-1}})$.

By taking in the above definition $A = \hat{k}^\times$, $B = \bar{\mathbb{F}}_q[[X]]^\times$, using the action defined in (5.1), we get a semi-direct product

$$\hat{k}^\times \ltimes \bar{\mathbb{F}}_q[[X]]^\times$$

Definition. Let $d \geq 1$. The group $\mathfrak{G}_d(k, \phi)$ is the subgroup of $\hat{k}^\times \ltimes \bar{\mathbb{F}}_q[[X]]^\times$ defined by

$$\mathfrak{G}_d(k, \phi) = \Big\{(a, \xi) \in \hat{k}^\times \ltimes \bar{\mathbb{F}}_q[[X]]^\times : a = \pi^\nu u, \frac{\phi^d \xi}{\xi} = \frac{\{u\}(X)}{X}\Big\}$$

To prove that these are subgroups, let $(a,\xi),(b,\eta)\in\mathfrak{G}_d(k,\phi)$, $a=\pi^\nu u$, $b=\pi^\mu v$. Then

$$(a,\xi)(b,\eta)=(ab,\xi\cdot\phi^{-\nu}\eta\circ\{u\})$$

and

$$\begin{aligned}\frac{\phi^d(\xi\cdot\phi^{-\nu}\eta\circ\{u\})}{\xi\cdot\phi^{-\nu}\eta\circ\{u\}}&=\frac{\phi^d\xi}{\xi}\cdot\frac{\phi^d\phi^{-\nu}\eta\circ\{u\}}{\phi^{-\nu}\eta\circ\{u\}}=\frac{\phi^d\xi}{\xi}\cdot(\phi^{-\nu}\frac{\phi^d\eta}{\eta}\circ\{u\})=\\&=\frac{\{u\}(X)}{X}\cdot(\frac{\{v\}(X)}{X}\circ\{u\})=\frac{\{u\}(X)}{X}\cdot\frac{\{vu\}(X)}{\{u\}(X)}=\frac{\{uv\}(X)}{X}\end{aligned}$$

(note the use of the fact that ϕ acts trivially on $\{u\}\in\mathbb{F}_q[[X]]^\times$).

Proposition 5.4. *There is a short exact sequence*

$$1\to\mathbb{F}_{q^d}[[X]]^\times\to\mathfrak{G}_d(k,\phi)\to\hat{k}^\times\to 1\tag{5.6}$$

Proof. Define the mappings $i:\mathbb{F}_{q^d}[[X]]^\times\to\mathfrak{G}_d(k,\phi)$, $p:\mathfrak{G}_d(k,\phi)\to\hat{k}^\times$ by

$$\begin{aligned}i(\xi)&=(1,\xi)\\p((a,\xi))&=a\end{aligned}$$

Since $\xi\in\mathbb{F}_{q^d}[[X]]^\times$, $\phi^d\xi/\xi=1=\{1\}(X)/X$, hence $(1,\xi)\in\mathfrak{G}_d(k,\phi)$. Therefore i is well defined, and is clearly an injection.

Take $a\in\hat{k}^\times$ and write it as $a=\pi^\nu u$ for $\nu\in\hat{\mathbb{Z}}$, $u\in U$. By proposition 4.6, the mapping $\xi\mapsto\phi^d\xi/\xi$ is surjective in $\bar{\mathbb{F}}_q[[X]]^\times$, hence there is $\xi\in\bar{\mathbb{F}}_q[[X]]^\times$ for which

$$\frac{\phi^d\xi}{\xi}=\frac{\{u\}(X)}{X}$$

It follows that for such ξ, $(a,\xi)\in\mathfrak{G}_d(k,\phi)$, thus p is surjective.

Now, $\operatorname{Im} i=\operatorname{Ker} p$ follows from the fact that $(1,\xi)\in\mathfrak{G}_d(k,\phi)$ for $\xi\in\bar{\mathbb{F}}_q[[X]]^\times$ if and only if $\xi\in\mathbb{F}_{q^d}[[X]]^\times$. □

The last proposition states that $\mathfrak{G}_d(k,\phi)$ is an extension of $\hat{k}^\times$ by $\mathbb{F}_{q^d}[[X]]^\times$. By definition, the group $\mathfrak{G}_d(k,\phi)$ is embedded in the semi-direct product $\hat{k}^\times\ltimes\bar{\mathbb{F}}_q[[X]]^\times$. It seems natural to ask whether there is an isomorphism

$$\mathfrak{G}_d(k,\phi)\cong\hat{k}^\times\ltimes\mathbb{F}_{q^d}[[X]]^\times$$

preserving the first coordinate.

The answer to this question is negative, and the precise statement is given in the proposition below , which is an application of proposition 5.3.

Proposition 5.5. *The sequence in* (5.6) *is not split.*

Proof. Assume the contrary, i.e. that there is an injection $j : \hat{k}^\times \to \mathfrak{G}_d(k, \phi)$ such that $j \circ p$ is the identity map on $\hat{k}^\times$.

Let

$$\begin{aligned} j(\pi^d) &= (\pi^d, \xi) \\ j(u) &= (u, \eta_u) \qquad \text{for every } u \in U \end{aligned}$$

Since j is an injection and $\hat{k}^\times$ is abelian, the images $j(\pi^d)$ and $j(u)$ commute for every $u \in U$. Carrying out the multiplications, we get

$$(\pi^d u, \xi \cdot \phi^{-d}\eta_u) = (u\pi^d, \eta_u \cdot (\xi \circ \{u\}))$$

or equivalently,

$$\frac{\phi^{-d}\eta_u}{\eta_u} = \frac{\xi \circ \{u\}}{\xi} \tag{5.7}$$

for every $u \in U$.

Since $(u, \eta_u) \in \mathfrak{G}_d(k, \phi)$, we have

$$\frac{\phi^d \eta_u}{\eta_u} = \frac{\{u\}(X)}{X} \in \mathbb{F}_q[[X]]^\times$$

and therefore

$$\frac{\phi^{-d}\eta_u}{\eta_u} = \phi^{-d}\frac{\eta_u}{\phi^d\eta_u} = \frac{\eta_u}{\phi^d\eta_u} = \frac{X}{\{u\}(X)}$$

Substituting this in (5.7), we get that

$$\frac{X}{\{u\}(X)} = \frac{\xi \circ \{u\}}{\xi}$$

for every $u \in U$, or equivalently,

$$(\xi \cdot X) \circ \{u\} = \xi \cdot X \tag{5.8}$$

for every $u \in U$.

Observe that $\xi \in \mathbb{F}_{q^d}[[X]]^\times$. By proposition 5.3, the only power series $\zeta \in \mathbb{F}_{q^d}((X))^\times$ for which $\zeta \circ \{u\} = \zeta$ for every $u \in U$ are the constant series. But $\xi \cdot X$ cannot be constant, a contradiction.

This contradiction implies that our initial assumption of existence of such a j was false, hence the sequence (5.6) is not split. $\square$

Definition of $\mathfrak{G}(k, \phi)$

Let $d, e \geq 1$, and consider the mappings

$$\psi_{de,d} : \mathfrak{G}_{de}(k, \phi) \longrightarrow \mathfrak{G}_d(k, \phi)$$

defined by

$$\psi_{de,d} : (a, \xi) \longmapsto (a, \prod_{i=0}^{e-1} \phi^{i \cdot d} \xi)$$

Since

$$\frac{\phi^{de}(\xi)}{\xi} = \prod_{i=0}^{e-1} \frac{\phi^{d(i+1)}\xi}{\phi^{di}\xi} = \frac{\phi^d(\prod_{i=0}^{e-1} \phi^{di}\xi)}{\prod_{i=0}^{e-1} \phi^{di}\xi} \quad , \tag{5.9}$$

we get that

$$\frac{\phi^{de}\xi}{\xi} = \frac{\{u\}(X)}{X}$$

if and only if

$$\frac{\phi^d(\prod_{i=0}^{e-1} \phi^{di}\xi)}{\prod_{i=0}^{e-1} \phi^{di}\xi} = \frac{\{u\}(X)}{X}$$

hence the mappings $\psi_{de,d}$ are well-defined.

Using proposition 4.6, we prove

Proposition 5.6. *The mappings $\psi_{de,d}$ are surjective.*

Proof. Take $(a, \eta) \in \mathfrak{G}_d(k, \phi)$. By proposition 4.6, since $\eta \in \bar{\mathbb{F}}_q[[X]]^\times$, there is $\xi \in \bar{\mathbb{F}}_q[[X]]^\times$ such that

$$\eta = \prod_{i=0}^{e-1} \phi^{i \cdot d} \xi \quad .$$

By (5.9) we get that

$$\frac{\phi^{de}\xi}{\xi} = \frac{\phi^d \eta}{\eta}$$

hence $(a, \xi) \in \mathfrak{G}_{de}(k, \phi)$ and $\psi_{de,d}(a, \xi) = (a, \eta)$. □

Definition.

$$\mathfrak{G}(k, \phi) = \varprojlim \mathfrak{G}_d(k, \phi)$$

where the inverse limit is taken with respect to the homomorphisms $\psi_{de,d}$ for every $d, e \geq 1$.

For the proof of the following theorem, see [dS–K].

Theorem. *Let k be a local field.*

1. *A correspondence*

$$F/k \longmapsto M(F/k)$$

between metabelian extensions (soluble extensions of degree 2) and closed subgroups of $\mathfrak{G}(k,\phi)$ can be defined. This correspondence is one-to-one and onto, and

$$[F:k] = [\mathfrak{G}(k,\phi) : M(F/k)]$$

when $[F:k]$ is finite.

2. *There is a mapping*

$$\imath : \mathfrak{G}(k,\phi) \longmapsto \mathrm{Gal}((k^{ab})^{ab}/k)$$

which induces an isomorphism

$$\mathfrak{G}(k,\phi)/M(F/k) \cong \mathrm{Gal}(F/k)$$

for every metabelian extension F/k.

3. *Let $d \geq 1$. The following diagram is commutative:*

$$\begin{array}{ccccc}
\mathbb{F}_{q^d}[[X]]^\times & \longrightarrow & \mathfrak{G}_d(k,\phi) & \longrightarrow & \hat{k}^\times \\
\downarrow & & \downarrow \imath & & \downarrow \rho_k \\
\mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k^{ab}) & \longrightarrow & \mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k) & \longrightarrow & \mathrm{Gal}(k^{ab}/k)
\end{array}$$

where the top horizontal arrows are those of (5.6)*.*

6 Aim of the Work

This work deals with nilpotency problems concerning metabelian extensions of a local field k. Before stating the objectives of this work, we briefly review some of the basic concepts of nilpotency and pro-nilpotency.

Definition. Let G be a (topological) group, and let $H, K \leq G$ be subgroups. The *commutator group* $[H,K]$ of H,K is

$$[H,K] = \big\langle xyx^{-1}y^{-1} : x \in H, y \in K \big\rangle$$

where by $\langle A \rangle$ we mean the closed subgroup of G generated by A.

Definition. Let G be a group. The *lower central series* of G is defined as

$$G^0 = G$$
$$G^{n+1} = [G^n, G] \quad \text{for } n \geq 0$$

This is a decreasing sequence of closed subgroups of G.

Definition. A group G is *nilpotent* if there is an n for which $G^n = 1$. The least such n is called the *nilpotency class* of G.

In analogy to the lower central series, one can also define the *upper central series*. Let $\mathrm{Z}(G)$ denote the center of a group G. Then the groups $\mathrm{Z}_n(G)$ are defined inductively as

$$\mathrm{Z}_0(G) = 1$$
$$\mathrm{Z}_{n+1}(G)/\,\mathrm{Z}_n(G) = \mathrm{Z}(G/\,\mathrm{Z}_n(G))$$

If G is finite, then a well-known result states that a necessary and sufficient condition for G to be nilpotent is that there exists an n such that $\mathrm{Z}_n(G) = G$.

The Galois groups of (possibly infinite) field extensions are pro-finite groups, that is, inverse limits of finite groups. The notion of pro-nilpotent groups is defined similarly.

Definition. Let G be a group. G is *pro-nilpotent* if there exist nilpotent groups $\{H_i\}$ (and mappings $f_{ij} : H_j \to H_i$) such that

$$G = \varprojlim H_i$$

Here is a characterization of pro-nilpotent groups by their lower central series.

Lemma 6.1. *Let G be a group. Then G is pro-nilpotent if and only if*

$$\bigcap_{n\geq 1} G^n = 1$$

Proof. The groups G/G^n are nilpotent (since $(G/G^n)^n = 1$). It follows that if the intersection of the groups G^n is 1, then

$$G \cong \varprojlim G/G^n$$

is pro-nilpotent.

Conversely, assume that $G = \varprojlim H_i$. For every $n \geq 1$, the inverse limits $\varprojlim H_i^n$ are well-defined, since the homomorphisms

$$f_{ij} : H_j \longrightarrow H_i$$

map commutators to commutators, thus $f_{ij}(H_j^n) \subseteq H_i^n$. This argument shows also that these limits can be embedded canonically in G.

Since multiplication on G is defined by coordinates, we get that

$$G^n \subseteq \varprojlim H_i^n$$

Now, take g in the intersection of all G^n. Its i-th coordinate lies in the intersection of all H_i^n, which is 1, as H_i is nilpotent. Therefore $g = 1$ and the lemma follows. $\square$

Lemma 6.2. *Let G be a compact, pro-nilpotent group. Let $N \triangleleft G$ be a normal open subgroup. Then G/N is nilpotent.*

Proof. Since the groups G/G^n are nilpotent, it in enough to show that $G^n \leq N$ for some n.

Assume the contrary. Then for every $n \geq 1$, we can find $x_n \in G^n$ such that

$$x_n \in G^n \quad , \quad x_n \notin N$$

Since G is compact, there is a subsequence (x_{n_k}) of (x_n) which converges to $x \in G$. As G^n form a decreasing sequence of closed subgroups, we must have $x = 1$, thus $x \in N$. But this is a contradiction, since x is the limit point of $x_{n_k} \notin N$, and N is open. $\square$

Corollary. *Let G be compact, pro-nilpotent, and let $N \triangleleft G$ be a normal closed subgroup of finite index. Then G/N is nilpotent*

Proof. The conditions on N imply that N is open in G. $\square$

Definition. Let E/F be Galois extension of fields. E/F is called *pro-nilpotent* if $\mathrm{Gal}(E/F)$ is pro-nilpotent.

Since $\mathrm{Gal}(E/F)$ is the inverse limit of $\mathrm{Gal}(E'/F)$ where $[E' : F] < \infty$ contained in E, we get that E/F is pro-nilpotent if and only if every E'/F, for $[E' : F] < \infty$ contained in E, is nilpotent.

We ask the following basic questions:

- Let k be a local field. Is $(k^{ab})^{ab}/k$ pro-nilpotent ?
  More generally, we seek for a description of the maximal pro-nilpotent extension N of k contained in $(k^{ab})^{ab}/k$.

- We can also consider the maximal nilpotent extension of class n over k. A description of the maximal 2-step nilpotent over k can be found in [dS–K].

- A similar question is to find large pro-nilpotent extensions $(k^{ab})^{ab}/M$.

In part II we analyze the upper central series of the groups $\mathfrak{G}_d(k,\phi)$, which correspond to the extensions $(k_d^{nr}k_\pi)^{ab}/k$.

In section 7, we bound $\mathrm{Z}_1(\mathfrak{G}_d(k,\phi))$ from above and from below, and then we show that the center of a dense subgroup of $\mathfrak{G}_d(k,\phi)$ is isomorphic to $\mathbb{F}_q^\times$. This is done by using proposition 5.3.

In section 8, we use this approach to compute $\mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$. Again, we show that for the dense subgroup of $\mathfrak{G}_d(k,\phi)$ mentioned above, the next group in the upper central series is rather small.

To conclude this part, we prove in section 9 that the group $\mathfrak{G}(k,\phi)$ is centerless.

In part III we construct a family of metabelian extensions, which are not nilpotent if the order of the residue field of k is greater than 2. This enables us to show that for every non-ramified extension K/k, the extension $(Kk_\pi^0)^{ab}/K$ is not pro-nilpotent, where k_π^0/k is an extension of order $q-1$, generated by the root $\pi \cdot \omega_0 = 0$. This is an example for a relatively small extension which is not pro-nilpotent.

In section 10 we define these extensions, while in section 11 we compute their Galois groups over k and show that they can be described as extensions of $\mathrm{Aut}\, W_n$ by W_m, for $0 \leq m \leq n$. In section 12 we show that such groups are not nilpotent when $q > 2$, and their nilpotency class is $m+2$ (in particular, it can be arbitrarily large), when $q = 2$.

In part IV we analyze the lower central series. In section 13 we define, for $d \geq 1$, and a closed subgroup $H \leq U$, a sequence of subgroups $B_{d,\alpha}(H)$ of $\mathbb{F}_{q^d}[[X]]^\times$, and prove their important properties.

In section 14, we relate these subgroups to nilpotent extensions over a field L for which

$$\mathrm{Gal}(k^{ab}/L) = P \times H$$

where $P \leq \langle \pi^d \rangle^{\hat{\mathbb{Z}}}$. The main result of this section is that

$$\mathrm{Gal}((k_d^{nr}k_\pi)^{ab}/N_L) \cong B_{d,\omega}(H)$$

for the maximal pro-nilpotent extension N_L over L contained in $(k_d^{nr}k_\pi)^{ab}$.

In section 15 we use the results of the previous sections, for the specific cases $H = U_1$ and $H = U$. We prove that $B_{d,\omega}(U_1) = 1$ for every $d \geq 1$, and deduce that for every non-ramified extension K/k, the extension $(Kk_\pi)^{ab}/(Kk_\pi^0)$ is pro-nilpotent (note that the construction in part III implies that $(Kk_\pi)^{ab}/K$ is *not* pro-nilpotent).

Later, we show that for such K, the maximal pro-nilpotent extension over K contained in $(Kk_\pi)^{ab}$ equals the maximal pro-nilpotent extension over $k_{\pi,p}k^{nr}$ in $(Kk_\pi)^{ab}$, where $k_{\pi,p}k^{nr}$ is the class field of V, the group of $(q-1)$-th roots of unity in U. We also give a description of the groups $B_{d,\omega}(V)$, which correspond to such maximal pro-nilpotent extensions.

Part II
Upper Central Series

7 Computation of $\mathrm{Z}(\mathfrak{G}_d(k,\phi))$

In this section we present some results concerning $\mathrm{Z}(\mathfrak{G}_d(k,\phi))$. We do not have yet an exact description of the center. However, we do have results that enable us to "bound" it from above and from below. In particular, as we see later, we can compute $\mathrm{Z}(\mathfrak{G}(k,\phi))$ using these results.

Throughout this section, we fix $d \geq 1$ and consider the group $\mathfrak{G}_d(k,\phi)$.

Upper Bounds

We start by defining a group which will serve as an upper bound for the center.

Definition.

$$\mathfrak{H}_d(k,\phi) = \left\{ (a,\xi) \in \mathfrak{G}_d(k,\phi) \,:\, a \in \langle \pi^d \rangle^{\hat{\mathbb{Z}}}, \xi \in \mathbb{F}_q[[X]]^\times \right\}$$

It is straightforward to verify that $\mathfrak{H}_d(k,\phi)$ is actually a subgroup of $\mathfrak{G}_d(k,\phi)$. The following propositions shed some light on the structure of $\mathfrak{H}_d(k,\phi)$.

Proposition 7.1. $\mathfrak{H}_d(k,\phi) \cong \hat{\mathbb{Z}} \times \mathbb{F}_q[[X]]^\times$.

Proof. Take two elements $(\pi^{d\nu},\xi),(\pi^{d\mu},\eta)$ in $\mathfrak{H}_d(k,\phi)$. Then, since ϕ acts trivially on $\mathbb{F}_q[[X]]^\times$, we have

$$(\pi^{d\nu},\xi)(\pi^{d\mu},\eta) = (\pi^{d(\nu+\mu)},\xi\eta) \tag{7.1}$$

Thus the mapping $(\pi^{d\nu},\xi) \mapsto (\nu,\xi)$ is a homomorphism from $\mathfrak{H}_d(k,\phi)$ to $\hat{\mathbb{Z}} \times \mathbb{F}_q[[X]]^\times$. It is clear that this homomorphism is injective. It is also surjective since every $\nu \in \hat{\mathbb{Z}}$ and $\xi \in \mathbb{F}_q[[X]]^\times$ define an element $(\pi^{d\nu},\xi) \in \mathfrak{H}_d(k,\phi)$. $\square$

Proposition 7.2. *$\mathfrak{H}_1(k,\phi)$ is a maximal abelian subgroup of $\mathfrak{G}_1(k,\phi)$.*

Proof. Eq. (7.1) shows that $\mathfrak{H}_1(k,\phi)$ is abelian. To prove maximality, take an arbitrary element $(a,\xi) \in \mathfrak{G}_1(k,\phi)$ not belonging to $\mathfrak{H}_1(k,\phi)$. Write a as $\pi^\nu u$, where $u \neq 1$. Then

$$(1, 1+X)(a,\xi) = (a, (1+X)\cdot\xi)$$
$$(a,\xi)(1,1+X) = (a, \xi \cdot (1+\{u\}))$$

As $\{u\} \neq X$, the above equations show that (a,ξ) does not commute with $(1,1+X) \in \mathfrak{H}_1(k,\phi)$. $\square$

Remark. By metabelian local class field theory, one has

$$\mathfrak{H}_1(k,\phi) \cong \mathrm{Gal}(k_\pi^{ab}/k_\pi) \quad .$$

We now show that $\mathfrak{H}_d(k,\phi)$ serves as an upper bound for the center of $\mathfrak{G}_d(k,\phi)$.

Proposition 7.3. $\mathrm{Z}(\mathfrak{G}_d(k,\phi)) \subseteq \mathfrak{H}_d(k,\phi)$

Proof. The idea of the proof is rather simple; we take an element in the center, and see what conditions it satisfies. We prove that these conditions imply that the element is contained in $\mathfrak{H}_d(k,\phi)$.

Let $(a_0,\xi_0) \in \mathrm{Z}(\mathfrak{G}_d(k,\phi))$ be an element in the center. Write $a_0 = \pi^{\nu_0}u_0$ where $\nu_0 \in \hat{\mathbb{Z}}$ and $u_0 \in U$. We have, for every $(a,\xi) \in \mathfrak{G}_d(k,\phi)$,

$$(a_0,\xi_0)(a,\xi) = (a,\xi)(a_0,\xi_0)$$

Rewriting this equation after carrying out the multiplications for $a = \pi^\nu u$ ($\nu \in \hat{\mathbb{Z}}$, $u \in U$), we get

$$(a_0 a, \xi_0 \cdot (\phi^{-\nu_0}\xi \circ \{u_0\})) = (a a_0, \xi \cdot (\phi^{-\nu}\xi_0 \circ \{u\}))$$

or equivalently,

$$\frac{\phi^{-\nu_0}\xi \circ \{u_0\}}{\xi} = \frac{\phi^{-\nu}\xi_0 \circ \{u\}}{\xi_0} \tag{7.2}$$

Equation (7.2) holds for every element (a,ξ). We take $a=1$ and $a=\pi$ and examine the constraints imposed on (a_0,ξ_0).

Take $a=1$, so that $\nu=0$ and $u=1$. From the definition of $\mathfrak{G}_d(k,\phi)$, we see that in order to have $(1,\xi) \in \mathfrak{G}_d(k,\phi)$, $\xi \in \bar{\mathbb{F}}_q[[X]]^\times$ must satisfy

$$\frac{\phi^d\xi}{\xi} = 1$$

or equivalently, $\xi \in \mathbb{F}_{q^d}[[X]]^\times$. Substituting in (7.2), we get

$$\frac{\phi^{-\nu_0}\xi \circ \{u_0\}}{\xi} = 1 \tag{7.3}$$

Substitute $\xi = 1+X$ in (7.3). We get $\{u_0\} = X$, thus $u_0 = 1$ (recall that the map $u \mapsto \{u\}$ is an injection).

Rewriting (7.3), we obtain

$$\frac{\phi^{-\nu_0}\xi}{\xi} = 1 \quad .$$

As this is true for every $\xi \in \mathbb{F}_{q^d}[[X]]^\times$, we must have $\nu_0 \in d\hat{\mathbb{Z}}$.

Now write $\nu_0 = d\mu_0$ for $\mu_0 \in \hat{\mathbb{Z}}$. Eq. (7.2) gets the form

$$\frac{\phi^{-d\mu_0}\xi}{\xi} = \frac{\phi^{-\nu}\xi_0 \circ \{u\}}{\xi_0} \tag{7.4}$$

for every $(a,\xi) \in \mathfrak{G}_d(k,\phi)$.

Take $a = \pi$, so that $u = 1$ and $\nu = 1$. Similar reasoning as in the case of $a = 1$ shows that $(\pi,\xi) \in \mathfrak{G}_d(k,\phi)$ for every $\xi \in \mathbb{F}_{q^d}[[X]]^\times$. Substituting in (7.4), we see that

$$1 = \frac{\phi^{-1}\xi_0}{\xi_0}$$

hence $\xi_0 \in \mathbb{F}_q[[X]]^\times$.

We have shown that for every element (a_0,ξ_0) in the center, $a_0 \in \langle\pi^d\rangle^{\hat{\mathbb{Z}}}$ and $\xi_0 \in \mathbb{F}_q[[X]]^\times$, or in other words,

$$\mathrm{Z}(\mathfrak{G}_d(k,\phi)) \subseteq \mathfrak{H}_d(k,\phi) \quad .$$

$\square$

Remark. In the proof we used only the commutativity of (a_0,ξ_0) and (a,ξ) where $a \in \langle\pi\rangle$. This corresponds to commutativity with all automorphisms $\sigma \in \mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k_\pi)$.

We see from the proof of the preceding proposition, that a necessary and sufficient condition for an element $(a_0,\xi_0) \in \mathfrak{H}_d(k,\phi)$, $a_0 = \pi^{d\mu_0}$, to be in $\mathrm{Z}(\mathfrak{G}_d(k,\phi))$ is

$$\frac{\phi^{-d\mu_0}\xi}{\xi} = \frac{\xi_0 \circ \{u\}}{\xi_0} \tag{7.5}$$

for every $(u,\xi) \in \mathfrak{G}_d(k,\phi)$.

We now prove that the center of a dense subgroup of $\mathfrak{G}_d(k,\phi)$ is rather small.

Definition.

$$\mathfrak{F}_d(k,\phi) = \Big\{(a,\xi) \in \mathfrak{G}_d(k,\phi) : a = \pi^\nu u \text{ where } \nu \in \mathbb{Z},\, u \in U\Big\}$$

$\mathfrak{F}_d(k,\phi)$ is a subgroup of $\mathfrak{G}_d(k,\phi)$. It is also dense since $\langle\pi\rangle^{\mathbb{Z}}$ is dense in $\langle\pi\rangle^{\hat{\mathbb{Z}}}$.

Proposition 7.4. $\mathrm{Z}(\mathfrak{G}_d(k,\phi)) \cap \mathfrak{F}_d(k,\phi) = \Big\{(1,c) : c \in \mathbb{F}_q^\times\Big\}$

Proof. Let (a_0, ξ_0) be in the subgroup defined by the LHS. We already know that $a_0 = \pi^{d\mu_0}$ where $\mu_0 \in \hat{\mathbb{Z}}$ and $\xi_0 \in \mathbb{F}_q[[X]]^\times$.

Our assumption is that $d\mu_0 \in \mathbb{Z}$ is an integer. Since both (a_0, ξ_0) and $(a_0, \xi_0)^{-1}$ lie in the center, we may assume without loss of generality that $\mu_0 \geq 0$. Let $(u, \xi) \in \mathfrak{G}_d(k, \phi)$ be arbitrary. Since

$$\frac{\phi^d \xi}{\xi} = \frac{\{u\}(X)}{X} \in \mathbb{F}_q[[X]] \quad ,$$

we have

$$\frac{\phi^{dn} \xi}{\xi} = \frac{\{u\}(X)^n}{X^n} \qquad , \frac{\phi^{-dn} \xi}{\xi} = \frac{X^n}{\{u\}(X)^n}$$

for every $n \geq 0$. Rewriting (7.5), we obtain

$$\frac{X^{\mu_0}}{\{u\}(X)^{\mu_0}} = \frac{\xi_0 \circ \{u\}}{\xi_0}$$

and this is equivalent to

$$(X^{\mu_0} \xi_0) \circ \{u\} = X^{\mu_0} \xi_0 \quad , \tag{7.6}$$

this equation being true for every $u \in U$.

Proposition 5.3 states that the only power series $\lambda \in \mathbb{F}_q[[X]]$ that satisfy

$$\lambda \circ \{u\} = \lambda$$

for every $u \in U$, are the constant series. Applying this to our case, we get that μ_0 must be 0 and $\xi_0 \in \mathbb{F}_q^\times$.

On the other hand, it is easy to see that elements of the form $(1, c)$, $c \in \mathbb{F}_q^\times$, commute with every $(a, \xi) \in \mathfrak{G}_d(k, \phi)$. $\square$

Corollary. $\mathrm{Z}(\mathfrak{F}_d(k, \phi)) = \left\{(1, c) : c \in \mathbb{F}_q^\times\right\}$

Proof. It suffices to show that

$$\mathrm{Z}(\mathfrak{F}_d(k, \phi)) = \mathrm{Z}(\mathfrak{G}_d(k, \phi)) \cap \mathfrak{F}_d(k, \phi)$$

The inclusion $\supseteq$ follows from the fact that $\mathfrak{F}_d(k, \phi)$ is a subgroup $\mathfrak{G}_d(k, \phi)$. The reverse inclusion follows from the fact that an element which commutes with every element in a dense subgroup of a given group, lies in the center of that group. $\square$

Corollary. $\mathfrak{G}_d(k, \phi)' \cap \mathrm{Z}(\mathfrak{G}_d(k, \phi)) = \left\{(1, c) : c \in \mathbb{F}_q^\times\right\}$

Proof. Let $(a, \xi) \in \mathfrak{G}_d(k, \phi)'$. Then $a = 1$ and the result follows from the previous proposition. $\square$

Lower Bound

We already know that the center of the dense subgroup $\mathfrak{F}_d(k,\phi)$ is very small. We now show that this is not true for $\mathfrak{G}_d(k,\phi)$. The reason for that is the fact that power series $\xi \in \bar{\mathbb{F}}_q[[X]]^\times$ for which there is $a \in \hat{k}^\times$ with $(a,\xi) \in \mathfrak{G}_d(k,\phi)$ have their coefficients in a field much smaller than $\bar{\mathbb{F}}_q$. This enables us to find a large family of homomorphisms whose action on such power series is trivial. These homomorphisms correspond to elements in the center, as described below.

We begin by examining such power series ξ more carefully.

Notation.

$$\mathbb{F}_{q^{d(q-1)p^\infty}} = \bigcup_{n=0}^{\infty} \mathbb{F}_{q^{d(q-1)p^n}}$$

Lemma 7.5. *If $\xi \in \bar{\mathbb{F}}_q[[X]]^\times$ satisfies*

$$\frac{\phi^d \xi}{\xi} = \frac{\{u\}(X)}{X}$$

for a unit $u \in U$, then

$$\xi \in \mathbb{F}_{q^{d(q-1)p^\infty}}[[X]]^\times$$

More precisely, if

$$\xi = \sum_{i=0}^{\infty} a_i X^i \quad ,$$

then for every $n \geq 0$ and $i < p^n$, we have $a_i \in \mathbb{F}_{q^{d(q-1)p^n}}$.

Proof. $\{u\}(X)/X$ has a non-zero constant term, namely $u \bmod \mathfrak{p}$, thus it belongs to $\mathbb{F}_q[[X]]^\times$. By lemma 4.4, we have

$$\lim_{n\to\infty} \left(\frac{\{u\}(X)}{X}\right)^{(q-1)p^n} = 1$$

From the proof of that lemma, we deduce also that

$$\left(\frac{\{u\}(X)}{X}\right)^{(q-1)p^n} \equiv 1 \pmod{X^{p^n}}$$

for every $n \geq 0$.

Since $\phi^d \xi/\xi \in \mathbb{F}_q[[X]]$, we have

$$\frac{\phi^{d(q-1)p^n}\xi}{\xi} = \left(\frac{\phi^d \xi}{\xi}\right)^{(q-1)p^n} = \left(\frac{\{u\}(X)}{X}\right)^{(q-1)p^n} \equiv 1 \pmod{X^{p^n}}$$

Multiplying by ξ, we get

$$\phi^{d(q-1)p^n}\xi \equiv \xi \pmod{X^{p^n}}$$

As $\phi^{d(q-1)p^n}$ operates on ξ coefficient-wise, by examining the coefficients we conclude that for every $i < p^n$,

$$\phi^{d(q-1)p^n}(a_i) = a_i$$

or in other words, a_i lies in the fixed field of $\phi^{d(q-1)p^n}$.

$\phi(x) = x^q$ is the Frobenius automorphism of $\mathbb{F}_q$, therefore $\phi^{d(q-1)p^n}(x) = x^{q^{d(q-1)p^n}}$ is the Frobenius automorphism of $\mathbb{F}_{q^{d(q-1)p^n}}$, and $\mathbb{F}_{q^{d(q-1)p^n}}$ is its fixed field. Hence, for every $i < p^n$, $a_i \in \mathbb{F}_{q^{d(q-1)p^n}}$ and

$$\xi \in \mathbb{F}_{q^{d(q-1)p^\infty}}[[X]]^\times$$

$\square$

Corollary. *If $(a, \xi) \in \mathfrak{G}_d(k, \phi)$, then $\xi \in \mathbb{F}_{q^{d(q-1)p^\infty}}[[X]]^\times$.*

Proof. Write $a = \pi^\nu u$. Then $\phi^d\xi/\xi = \{u\}(X)/X$ and the result follows from the proposition. $\square$

Lemma 7.6. *Let ϕ be the Frobenius automorphism on $\bar{\mathbb{F}}_q/\mathbb{F}_q$. Then a necessary and sufficient condition for $\nu \in \hat{\mathbb{Z}}$ to satisfy $\phi^{d\nu} \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^{d(q-1)p^\infty}})$ is*

$$\nu \in (q-1)\hat{\mathbb{Z}} \cap \prod_{l \neq p} \mathbb{Z}_l \tag{7.7}$$

where $\hat{\mathbb{Z}} \cong \prod_l \mathbb{Z}_l$ canonically (l runs over all primes).

Proof. The statement $\phi^{d\nu} \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^{d(q-1)p^\infty}})$ is equivalent to the statement that $\phi^{d\nu}$ is the identity on every subfield $\mathbb{F}_{q^{d(q-1)p^n}}$ $(n \geq 0)$.

Now, $\phi^{d\nu}$ is the identity on $\mathbb{F}_{q^{d(q-1)p^n}}$ if and only if $(q-1)p^n \mid \nu$. Thus an equivalent condition on ν is to be divisible by every $(q-1)p^n$.

Assume first that ν is divisible by every $(q-1)p^n$. Since ν is divisible by $q-1$, we surely have $\nu \in (q-1)\hat{\mathbb{Z}}$. Now, view ν as a vector $(\nu_l)_l$ where l runs over all rational primes. As $p^n \mid \nu$ for every $n \geq 0$, we must have $\nu_p = 0$. Combining these conditions, we finally get

$$\nu \in (q-1)\hat{\mathbb{Z}} \cap \prod_{l \neq p} \mathbb{Z}_l$$

The above arguments can be reversed, hence the condition in (7.7) is also sufficient. $\square$

We can now prove

Proposition 7.7.

$$\mathrm{Z}(\mathfrak{G}_d(k,\phi)) \cap \left\{(a,\xi) \in \mathfrak{G}_d(k,\phi) : a = \pi^{d\nu} \textit{ for } \nu \in (q-1)\hat{\mathbb{Z}} \cap \prod_{l \neq p} \mathbb{Z}_l\right\} =$$
$$\left\{(a,c) : a = \pi^{d\nu} \textit{ for } \nu \in (q-1)\hat{\mathbb{Z}} \cap \prod_{l \neq p} \mathbb{Z}_l \,,\, c \in \mathbb{F}_q^\times\right\} \quad (7.8)$$

Proof. Let (a_0, ξ_0) be an element in the LHS of (7.8). By proposition 7.3, $a_0 = \pi^{d\nu_0}$ for $\nu_0 \in \hat{\mathbb{Z}}$, and $\xi_0 \in \mathbb{F}_q[[X]]^\times$.

(a_0, ξ_0) satisfies (7.5), that is, for each $(u, \xi) \in \mathfrak{G}_d(k,\phi)$ where $u \in U$, the following equality holds:

$$\frac{\phi^{-d\nu_0}\xi}{\xi} = \frac{\xi_0 \circ \{u\}}{\xi_0} \quad (7.9)$$

Take $(u,\xi) \in \mathfrak{G}_d(k,\phi)$. By lemma 7.5, $\xi \in \mathbb{F}_{q^{d(q-1)p^\infty}}[[X]]^\times$. Now, lemma 7.6 states that $\phi^{d\nu_0}$ is the identity of $\mathbb{F}_{q^{d(q-1)p^\infty}}$, so that the LHS of (7.9) equals 1. Thus

$$1 = \frac{\xi_0 \circ \{u\}}{\xi_0}$$

for every $u \in U$. Proposition 5.3 now yields that $\xi_0 \in \mathbb{F}_q^\times$ is a constant series.

As (7.9) is also a sufficient condition for being in the center, we see that elements belonging to the RHS of (7.8) lie in the center. □

Corollary. $\mathrm{Z}(\mathfrak{G}_d(k,\phi))$ *contains the subgroup*

$$\left\{(a,c) \in \mathfrak{G}_d(k,\phi) \ : \ a = \pi^{d\nu} \textit{ for } \nu \in (q-1)\hat{\mathbb{Z}} \cap \prod_{l \neq p} \mathbb{Z}_l \,,\, c \in \mathbb{F}_q^\times\right\}$$

Proof. Clear. □

8 Computation of $\mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$

In this section, we present some results regarding the computation of the second element in the upper central series of $\mathfrak{G}_d(k,\phi)$. Throughout this section we keep $d \geq 1$ fixed.

Proposition 8.1. *Let G be a group and let $z \in \mathrm{Z}_2(G)$. Then the mapping*

$$\rho_z(g) = [z, g]$$

is a homomorphism $\rho_z : G \longrightarrow G' \cap \mathrm{Z}(G)$.

Proof. Let $\bar{g}$ be the image of g under the canonical homomorphism from G to $G/\mathrm{Z}(G)$. Since

$$\mathrm{Z}_2(G)/\mathrm{Z}(G) = \mathrm{Z}(G/\mathrm{Z}(G))$$

and $z \in \mathrm{Z}_2(G)$, we have $\bar{z}\bar{g} = \bar{g}\bar{z}$ for every $g \in G$, or equivalently, $\overline{[z,g]} = 1$, thus $\rho_z(g) \in \mathrm{Z}(G)$. Since $\rho_z(g)$ is a commutator, it is surely in G'.

Now,

$$\begin{aligned}[z, gh] &= zghz^{-1}h^{-1}g^{-1} = \\ &= zgz^{-1}g^{-1}gzhz^{-1}h^{-1}g^{-1} = [z,g][z,h]^g = [z,g][z,h]\end{aligned}$$

because $[z,h] \in \mathrm{Z}(G)$ is invariant under conjugation. Similarly,

$$[z, g^{-1}] = zg^{-1}z^{-1}g = (g^{-1}zgz^{-1})^{-1} = [z,g]^{-g^{-1}} = [z,g]^{-1}$$

so that $\rho_z : G \longrightarrow G' \cap \mathrm{Z}(G)$ is a homomorphism. ∎

Fix $(a_0, \xi_0) \in \mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$. The previous proposition states that there is a homomorphism

$$\rho_{(a_0,\xi_0)} : \mathfrak{G}_d(k,\phi) \longrightarrow \mathfrak{G}_d(k,\phi)' \cap \mathrm{Z}(\mathfrak{G}_d(k,\phi))$$

From the corollary after proposition 7.4, the image of this homomorphism is contained in the subgroup $\{(1,c) : c \in \mathbb{F}_q^\times\}$. We can therefore write

$$\rho_{(a_0,\xi_0)}(a,\xi) = (1, c_{(a,\xi)})$$

for every $(a,\xi) \in \mathfrak{G}_d(k,\phi)$.

Let us now exploit some of the properties of the homomorphism $c : (a,\xi) \mapsto c_{(a,\xi)}$. Recall that by definition of ρ,

$$[(a_0,\xi_0),(a,\xi)] = (1, c_{(a,\xi)})$$

Carrying out the multiplications, substituting $a_0 = \pi^{\nu_0}u_0$ and $a = \pi^{\nu}u$ where $u_0, u \in U$, we get

$$\frac{\xi_0}{\phi^{-\nu}\xi_0 \circ \{u\}} \cdot \frac{\phi^{-\nu_0}\xi \circ \{u_0\}}{\xi} = c_{(a,\xi)} \tag{8.1}$$

Lemma 8.2. *Let* $(1,\xi) \in \mathfrak{G}_d(k,\phi)$. *Then* $c_{(1,\xi)} = 1$.

Proof. As $a = 1$, equation (8.1) has the form

$$\frac{\phi^{-\nu_0}\xi \circ \{u_0\}}{\xi} = c_{(1,\xi)} \tag{8.2}$$

Substitute $\xi = X + 1$ in (8.2). We get

$$\frac{1 + \{u_0\}(X)}{1 + X} = c_{(1,1+X)} \tag{8.3}$$

From (8.3) we deduce that $c_{(1,1+X)} = 1$ and therefore $\{u_0\} = X$. Rewriting (8.2), we see that

$$\frac{\phi^{-\nu_0}\xi}{\xi} = c_{(1,\xi)}$$

Now let ξ be arbitrary and let $\xi_1 = 1 + X\xi$. Substituting, we get

$$c_{(1,1+X\xi)} = \frac{\phi^{-\nu_0}\xi_1}{\xi_1} = \frac{1 + X\phi^{-\nu_0}\xi}{1 + X\xi} = \frac{1 + c_{(1,\xi)}X\xi}{1 + X\xi}$$

hence $1 = c_{(1,1+X\xi)} = c_{(1,\xi)}$. □

Corollary. *$c_{(a,\xi)}$ does not depend on ξ.*

Proof. Let $(a,\xi), (a,\xi')$ be two elements of $\mathfrak{G}_d(k,\phi)$. Then

$$(1, \frac{\xi'}{\xi})(a,\xi) = (a,\xi')$$

and therefore

$$c_{(1,\frac{\xi'}{\xi})}c_{(a,\xi)} = c_{(a,\xi')}$$

and the result follows from $c_{(1,\frac{\xi'}{\xi})} = 1$. □

Corollary. *Let $(a_0, \xi_0) \in \mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$. Then $a_0 \in \langle \pi^d \rangle^{\hat{\mathbb{Z}}}$.*

Proof. Write $a_0 = \pi^{\nu_0}u_0$ for $\nu_0 \in \hat{\mathbb{Z}}$, $u_0 \in U$. In the proof of lemma 8.2 we saw that $\{u_0\} = X$, thus $u_0 = 1$. Moreover, by that lemma we also get that $c_{(1,\xi)} = 1$ for every $(1,\xi) \in \mathfrak{G}_d(k,\phi)$. Therefore

$$\frac{\phi^{-\nu_0}\xi}{\xi} = 1$$

for every $\xi \in \mathbb{F}_{q^d}[[X]]^\times$, hence $\nu_0 \in d\hat{\mathbb{Z}}$. □

Remark. One can also prove that $c_{(1,\xi)} = 1$ by metabelian class field theory, as follows. We have a commutative diagram

$$\begin{array}{ccccc}
\mathbb{F}_{q^d}[[X]]^\times & \longrightarrow & \mathfrak{G}_d(k,\phi) & \longrightarrow & \hat{k}^\times \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Gal}((k_\pi k_d^{nr})^{ab})/k^{ab}) & \longrightarrow & \mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k) & \longrightarrow & \mathrm{Gal}(k^{ab}/k)
\end{array}$$

Since k^{ab}/k is the maximal abelian extension over k, we must have that $\mathfrak{G}_d(k,\phi)' = \left\{(1,\xi) : \xi \in \mathbb{F}_{q^d}[[X]]^\times\right\}$. Now, as $c : \mathfrak{G}_d(k,\phi) \to \mathbb{F}_q^\times$ is an homomorphism into an abelian group, its kernel contains the commutator subgroup.

Since $c_{(a,\xi)}$ does not depend on ξ, we can regard c as an homomorphism $c : \hat{k}^\times \to \mathbb{F}_q^\times$, and rewrite (8.1) as

$$\frac{\phi^{-d\mu_0}\xi}{\xi} \cdot \frac{\xi_0}{\phi^{-\nu}\xi_0 \circ \{u\}} = c_a \tag{8.4}$$

for $(\pi^{d\mu_0}, \xi_0) \in \mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$ and every $(a,\xi) \in \mathfrak{G}_d(k,\phi)$, where $a = \pi^\nu u$.

Lemma 8.3. *$c : U \to \mathbb{F}_q^\times$ is continuous.*

Proof. Let $u_n \to u$. For each n, choose ξ_n such that $(u_n, \xi_n) \in \mathfrak{G}_d(k,\phi)$. Since $\bar{\mathbb{F}}_q[[X]]^\times$ is compact, we can find a convergent subsequence of $\{\xi_n\}$. To simplify notation, we call it again $\{\xi_n\}$.

Since $\xi_n \to \xi$, and since $u \mapsto \{u\}$ is continuous, we get that

$$\frac{\{u\}(X)}{X} = \lim_{n\to\infty} \frac{\{u_n\}(X)}{X} = \lim_{n\to\infty} \frac{\phi^d \xi_n}{\xi_n} = \frac{\phi^d \xi}{\xi}$$

therefore $(u,\xi) \in \mathfrak{G}_d(k,\phi)$.

Now, by (8.4),

$$c_u = \frac{\phi^{-d\mu_0}\xi}{\xi} \cdot \frac{\xi_0}{\xi_0 \circ \{u\}} = \lim_{n\to\infty} \frac{\phi^{-d\mu_0}\xi_n}{\xi_n} \cdot \lim_{n\to\infty} \frac{\xi_0}{\xi_0 \circ \{u_n\}} = \lim_{n\to\infty} c_{u_n}$$

□

Lemma 8.4. $U_1 \leq \operatorname{Ker} c$.

Proof. Let $u \in U_1$. Then $u^{q^n} \to 1$. But since $c(u) \in \mathbb{F}_q^\times$,

$$c(u^{q^n}) = c(u)^{q^n} = c(u)$$

and by continuity of c, $c(u) = c(1) = 1$. □

As in the case of the center, we can now prove that the intersection of $\mathrm{Z}_2(\mathfrak{G}_d(k,\phi))$ and the dense subgroup $\mathfrak{F}_d(k,\phi)$ is quite small.

Proposition 8.5. $\mathrm{Z}_2(\mathfrak{G}_d(k,\phi)) \cap \mathfrak{F}_d(k,\phi) \subseteq \left\{(1,x) : x \in \mathbb{F}_{q^d}^\times\right\}$

Proof. Rewriting (8.4) for (u,ξ) when $u \in U_1$, and using lemma 8.4, we get

$$\frac{\phi^{-d\mu_0}\xi}{\xi} \cdot \frac{\xi_0}{\xi_0 \circ \{u\}} = 1$$

But this is precisely the condition in (7.5).

Now the proposition follows by repeating the argument in the proof of proposition 7.4, replacing U with the group U_1 when using proposition 5.3. □

Corollary. $\mathrm{Z}_2(\mathfrak{G}_1(k,\phi)) \cap \mathfrak{F}_1(k,\phi) = \mathrm{Z}(\mathfrak{F}_1(k,\phi))$.

Proof. Apply the proposition with $d = 1$, and use the corollary after proposition 7.4. $\square$

9 Computation of $\mathrm{Z}(\mathfrak{G}(k,\phi))$

In this section, we compute $\mathrm{Z}(\mathfrak{G}(k,\phi))$ using the results we have obtained on $\mathrm{Z}(\mathfrak{G}_d(k,\phi))$. As $\mathfrak{G}(k,\phi)$ is defined as an inverse limit of $\mathfrak{G}_d(k,\phi)$, considerations involving such limits come into play.

We start by computing the inverse limit of the groups $\mathfrak{H}_d(k,\phi)$.

Proposition 9.1. $\varprojlim_d \mathfrak{H}_d(k,\phi) = 1$.

Proof. First we show that the inverse limit is well defined. To do this, we prove that for every $d, e \geq 1$, we have

$$\psi_{de,d}(\mathfrak{H}_{de}(k,\phi)) \subseteq \mathfrak{H}_d(k,\phi)$$

Take an element $(a,\xi) \in \mathfrak{H}_{de}(k,\phi)$. We have to verify that

$$(a, \prod_{i=0}^{e-1} \phi^{di}\xi) \in \mathfrak{H}_d(k,\phi) \ ,$$

but this is clear from the definition, since $\langle \pi^{de} \rangle^{\hat{\mathbb{Z}}} \subseteq \langle \pi^{d} \rangle^{\hat{\mathbb{Z}}}$ and $\xi \in \mathbb{F}_q[[X]]^\times$.

Now, take an element $(a_d, \xi_d)_d \in \varprojlim_d \mathfrak{H}_d(k,\phi)$, and fix $d \geq 1$. By definition of the maps $\psi_{de,d}$, we have (for the first coordinate)

$$a_{de} = a_d$$

for every $e \geq 1$, where $a_{de} \in \langle \pi^{de} \rangle^{\hat{\mathbb{Z}}}$. Thus

$$a_d \in \bigcap_{e \geq 1} \langle \pi^{de} \rangle^{\hat{\mathbb{Z}}} = \{1\}$$

Considering the second coordinate, we have, for every $e \geq 1$,

$$\xi_d = \prod_{i=0}^{e-1} \phi^{di}\xi_{de} = \xi_{de}^e \tag{9.1}$$

where the latter equality follows from the fact that $\xi_{de} \in \mathbb{F}_q[[X]]^\times$. Let $n \geq 0$, and choose $e = (q-1)p^n$. Substituting for e in (9.1), we get that

$$\xi_d = \xi_{d(q-1)p^n}^{(q-1)p^n}$$

Since $\eta^{(q-1)p^n} \in 1 + X^{p^n}\mathbb{F}_q[[X]]$ for every $\eta \in \mathbb{F}_q[[X]]^\times$, we see that $\xi_d \in 1 + X^{p^n}\mathbb{F}_q[[X]]$. As this is true for every $n \geq 0$, we finally get $\xi_d = 1$.

Now, since $a_d = 1$ and $\xi_d = 1$ for every $d \geq 1$, the proposition follows. $\square$

We now prove a simple proposition which connects the center of an inverse limit of groups with the inverse limit of the centers.

Proposition 9.2. *Let I be a partially ordered set, and let $\{G_i\}$ be a family of groups indexed by I. Suppose that we have homomorphisms*

$$f_{ij} : G_i \longrightarrow G_j$$

for every $i > j$, and define $\varprojlim G_i$ in the usual manner. Set also $Z_i = \mathrm{Z}(G_i)$.
If the above homomorphisms are surjective then we have the following:

(i) $f_{ij}(Z_i) \subseteq Z_j$ *for every $i > j$. Hence $\varprojlim Z_i$ is defined and can be canonically embedded in $\varprojlim G_i$.*

(ii) $\mathrm{Z}(\varprojlim G_i) = \varprojlim Z_i$.

Proof. Fix $i > j$, and let $z_i \in Z_i$. To show that $f_{ij}(z_i) \in Z_j$, take $g_j \in G_j$. Since f_{ij} is surjective, we can find $g_i \in G_i$ for which $g_j = f_{ij}(g_i)$. Now,

$$f_{ij}(z_i)g_j \;=\; f_{ij}(z_i)f_{ij}(g_i) \;=\; f_{ij}(z_ig_i) \;=\; f_{ij}(g_iz_i) \;=\; g_jf_{ij}(z_i) \quad (9.2)$$

where we used the fact that z_i commutes with g_i. Since (9.2) is true for every $g_j \in G_j$, we have $f_{ij}(z_i) \in Z_j$.

We may now define $\varprojlim Z_i$ using the maps f_{ij}. In particular, $(z_i)_i \in \varprojlim Z_i$ can be viewed as an element of $\varprojlim G_i$ (since $z_i \in G_i$ and $f_{ij}(z_i) = z_j$ for every $i > j$).

To prove the second assertion of the proposition, take $z \in \mathrm{Z}(\varprojlim G_i)$, and write it as $z = (z_i)_i$, where $z_i \in G_i$. Since the maps f_{ij} are surjective, the projections from $\varprojlim G_i$ to each G_i are surjective. Take $i \in I$ and $g_i \in G_i$. We can find $g \in \varprojlim G_i$ whose i-th coordinate is g_i. Since $zg = gz$, we surely have $z_ig_i = g_iz_i$. As this is true for every $g_i \in G_i$ and every $i \in I$, we get $z_i \in Z_i$ for every i, hence

$$\mathrm{Z}(\varprojlim G_i) \subseteq \varprojlim Z_i$$

To prove the opposite inclusion, take $z = (z_i)_i \in \varprojlim Z_i$ and let $g = (g_i)_i \in \varprojlim G_i$ be arbitrary. Since $z_ig_i = g_iz_i$ for every i, we get $zg = gz$, hence $z \in \mathrm{Z}(\varprojlim G_i)$ and the proposition is proven.

$\square$

With proposition 9.2 at hand, we can now state and prove the main theorem of this section.

Theorem 9.3. $\mathrm{Z}(\mathfrak{G}(k,\phi)) = 1$.

Proof. $\mathfrak{G}(k,\phi) = \varprojlim_d \mathfrak{G}_d(k,\phi)$ is defined using the homomorphisms

$$\psi_{de,d} : \mathfrak{G}_{de}(k,\phi) \to \mathfrak{G}_d(k,\phi)$$

which from proposition 5.6 are known to be surjective.

Applying proposition 9.2, we get that

$$\mathrm{Z}(\mathfrak{G}(k,\phi)) = \varprojlim_d \mathrm{Z}(\mathfrak{G}_d(k,\phi))$$

But from proposition 7.3 we have $\mathrm{Z}(\mathfrak{G}_d(k,\phi)) \subseteq \mathfrak{H}_d(k,\phi)$, and proposition 9.1 states that $\varprojlim_d \mathfrak{H}_d(k,\phi) = 1$.

Thus $\varprojlim_d \mathrm{Z}(\mathfrak{G}_d(k,\phi)) = 1$, and

$$\mathrm{Z}(\mathfrak{G}(k,\phi)) = 1 \quad .$$

□

Corollary. *The center of* $\mathrm{Gal}((k^{ab})^{ab}/k)$ *is trivial.*

Proof. $\mathrm{Gal}((k^{ab})^{ab}/k) = \mathfrak{G}(k,\phi)$. □

Part III

Explicit Constructions

In this part, we will construct a family of extensions of a local field k which are metabelian and non-nilpotent (in the case where the order of the residue field of k is greater than 2). We later use these extensions to show that some metabelian extensions are not pro-nilpotent over k.

The construction is analogous to the construction of Kummer extensions over a field F. When constructing Kummer extensions, we first attach an n-th root of unity, ζ_n, to F, and then look at the extension $F(\alpha_n, \zeta_n)/F$ where $\alpha_n^n = a$ for $a \in F$. Here we replace the operation of raising to the n-th power by applying an endomorphism $[\pi^{n+1}]$ derived from a Lubin-Tate power series, in a way described below.

This analogy suggests the name "Kummer-Lubin-Tate" for the extensions that we construct.

10 Definition of the Extensions $k(\alpha_n, \omega_n)/k$

As before, (k, ν) is a local field with a ring of integers $\mathfrak{o}$, a maximal ideal $\mathfrak{p}$ and residue field $\mathbb{F}_q$. Let $\pi \in k$ be a prime element, and $h(X)$ be a Lubin-Tate power series with respect to π (see section 2), that is,

$$h(X) \equiv \pi X \pmod{\deg 2} \tag{10.1}$$

$$h(X) \equiv X^q \pmod{\mathfrak{p}} \tag{10.2}$$

Assume also that $h(X)$ is a *polynomial* of degree q in $\mathfrak{o}[X]$.

Let $F_h(X,Y) \in \mathfrak{o}[[X,Y]]$ be the group law that corresponds to h. Recall that for every $a \in \mathfrak{o}$ we have a power series $[a]$ which is an endomorphism of F_h. By $h \in \mathfrak{o}[[X]]$ and (10.1) we deduce that $[\pi] = h$, and therefore $[\pi^n] = h \circ \cdots \circ h$ (composition n times).

Let Ω be an algebraic closure of k, and let μ be an extension of ν to Ω. Let $\bar{\Omega}$ be a completion of Ω with valuation $\bar{\mu}$, and $\mathfrak{p}_{\bar{\Omega}}$ be the maximal ideal in $\bar{\Omega}$ (i.e. the set of elements with positive valuation). Recall that we can define an $\mathfrak{o}$-module structure on $\mathfrak{p}_{\bar{\Omega}}$. Let W_n, for $n \geq 1$, be the π^{n+1}-torsion submodules.

From now on we assume that ω_n, for $n \geq 0$, have been fixed once and for all as generators of the corresponding modules W_n.

Throughout this part, we fix a prime element $a \in k$. For every $n \geq 0$, we choose $\alpha_n \in \Omega$ such that

$$[\pi^{n+1}](\alpha_n) = a \tag{10.3}$$

Such a choice can be made, since Ω is algebraically closed, and $[\pi^n]$ are polynomials.

First we show that $\alpha_n \in \mathfrak{p}_\Omega$. In order to do that, we need a general lemma on the roots of Eisenstein polynomials.

Lemma 10.1. *Let $f \in \mathfrak{o}[X]$ be an Eisenstein polynomial of degree m, $f = X^m + c_{m-1}X^{m-1} + \cdots + c_1X + c_0$, and let α be a root of f in Ω.*

Then the extension $k(\alpha)/k$ is totally ramified,

$$[k(\alpha) : k] = m$$

and α is a prime in $k(\alpha)$.

Proof. It is known that an Eisenstein polynomial is irreducible, therefore $[k(\alpha) : k] = m$. Since $\mathrm{N}_{k(\alpha)/k}(\alpha) = \pm c_0$, we see that

$$m\mu(\alpha) = \mu(c_0) \tag{10.4}$$

(because conjugate elements over k have the same valuation).

Now, the fact that f is Eisenstein implies that $\nu(c_0) = 1$, hence $\mu(k^\times) = \mu(c_0)\mathbb{Z}$. It is also evident that $\mu(k(\alpha)^\times) \subseteq \mu(\alpha)\mathbb{Z}$. Combining these and (10.4), we get for the ramification index $e(k(\alpha)/k)$,

$$\begin{aligned}[k(\alpha) : k] \geq e(k(\alpha)/k) = [\mu(k(\alpha)^\times) : \mu(k^\times)] \geq \\ \geq [\mu(\alpha)\mathbb{Z} : \mu(c_0)\mathbb{Z}] = \frac{\mu(c_0)}{\mu(\alpha)} = m = [k(\alpha) : k]\end{aligned}$$

so that $k(\alpha)/k$ is totally ramified of degree m, and all inequalities are in fact equalities. In particular, as $\mu(k(\alpha)^\times) = \mu(\alpha)\mathbb{Z}$, we also get that α is a prime element of $k(\alpha)$. □

Lemma 10.2. *Let $n \geq 0$. Then the extension $k(\alpha_n)/k$ is totally ramified of degree q^{n+1}, and α_n is a prime in that extension.*

Proof. It suffices to check that the polynomial

$$[\pi^{n+1}](X) - a$$

is Eisenstein of degree q^{n+1}.

Recall that $[\pi^{n+1}] = h \circ h \circ \cdots \circ h$. The degree of h is q, thus the degree of the $n+1$-th composition is q^{n+1}. In addition, as h is divisible by X, the same is true for the composition. By (10.2) we also get that

$$[\pi^{n+1}](X) \equiv X^{q^{n+1}} \pmod{\mathfrak{p}}$$

We still have to show that the constant term of $[\pi^{n+1}] - a$ is a prime of k. But this is clear, as a is a prime and $[\pi^{n+1}]$ is divisible by X. □

Lemma 10.3. *Let α_n be defined as above and let $\sigma \in \mathrm{Gal}(\Omega/k)$. Then $\sigma(\alpha_n)$ is another solution of (10.3) and $\alpha_n \dot{-} \sigma(\alpha_n) \in W_n$.*

Proof. Since $[\pi^{n+1}] - a$ has its coefficients in k, it is clear that the image under σ of a solution to (10.3) is also a solution of that equation. Now,

$$\pi^{n+1} \cdot (\alpha_n \dot{-} \sigma(\alpha_n)) = \pi^{n+1} \cdot \alpha_n \dot{-} \pi^{n+1} \cdot \sigma(\alpha_n) = a \dot{-} a = 0$$

hence $\alpha_n \dot{-} \sigma(\alpha_n) \in W_n$. $\square$

Proposition 10.4. *Let $m, n \geq 0$ and assume that $m \geq n$. Then the extension $k(\alpha_n, \omega_m)/k$ is Galois.*

Proof. It suffices to show that $k(\alpha_n, \omega_m)$ is left invariant under arbitrary $\sigma \in \mathrm{Gal}(\Omega/k)$. For such σ we have $\sigma(\omega_m) \in W_m$.

By the previous lemma, if we let $\omega = \sigma(\alpha_n) \dot{-} \alpha_n$, then $\omega \in W_n$. Since $m \geq n$, it follows that $W_n \subseteq W_m \subseteq k(\omega_m)$. In particular, $\omega \in k(\omega_m)$. As $k(\alpha_n, \omega_m)/k$ is finite, it is also closed in $\bar{\Omega}$, hence

$$\sigma(\alpha_n) = \alpha_n \dot{+} \omega \in k(\alpha_n, \omega_m)$$

and the proposition follows. $\square$

We shall examine later in detail the Galois groups of the extensions $k(\alpha_n, \omega_n)/k$ for every $n \geq 0$, and show that these extensions are examples of a metabelian non-nilpotent extensions. At the moment, we present a simple result for the case $n = 0$, whose proof does not involve any group considerations.

Proposition 10.5. *The extension $k(\alpha_0, \omega_0)/k$ is totally ramified of degree $q(q-1)$.*

Proof. We already know that the extension $k(\omega_0)/k$ is totally ramified of degree $q-1$ and that ω_0 is prime. Thus

$$\mu(\omega_0) = \frac{1}{q-1} \tag{10.5}$$

By lemma 10.2, $k(\alpha_0)/k$ is totally ramified of degree q and α_0 is prime element. Hence

$$\mu(\alpha_0) = \frac{1}{q} \tag{10.6}$$

Now take $\omega_0/\alpha_0 \in k(\alpha_0, \omega_0)$. By (10.5) and (10.6),

$$\mu(\frac{\omega_0}{\alpha_0}) = \left(\frac{1}{q-1} - \frac{1}{q}\right) = \frac{1}{q(q-1)}$$

thus $e(k(\alpha_0, \omega_0)/k) \geq q(q-1)$.

Since $[k(\omega_0) : k] = q - 1$ and $[k(\alpha_0) : k] = q$, we must have $[k(\alpha_0, \omega_0) : k] \leq q(q-1)$. Combining these inequalities, we get

$$q(q-1) \geq [k(\alpha_0, \omega_0) : k] \geq e(k(\alpha_0, \omega_0)/k) \geq q(q-1)$$

and all inequalities are in fact equalities. We deduce that the extension $k(\alpha_0, \omega_0)/k$ is totally ramified of degree $q(q-1)$. $\square$

11 The Groups $\mathrm{Gal}(k(\alpha_n, \omega_n)/k)$

In this section we describe the groups $\mathrm{Gal}(k(\alpha_n, \omega_n)/k)$ for $n \geq 0$.

We use the construction defined in section 5, (5.4) and (5.5) for the groups $A = \mathrm{Aut}\, W_n$ and $B = W_m$ where $m \leq n$ (note that by $\mathrm{Aut}\, W_n$ we mean automorphisms that preserve not only the additive structure of W_n, but also its $\mathfrak{o}$-module structure.)

Definition. Let $m, n \geq 0$, $m \leq n$. The group $\mathrm{Aut}\, W_n \ltimes W_m$ is defined as

$$\mathrm{Aut}\, W_n \ltimes W_m = \Big\{(\varepsilon, \omega) : \varepsilon \in \mathrm{Aut}\, W_n, \omega \in W_m\Big\}$$

where multiplication of two elements (ε, ω) and (ε', ω') is defined as

$$(\varepsilon, \omega)(\varepsilon', \omega') = (\varepsilon\varepsilon', \omega \dotplus \varepsilon(\omega'))$$

Note that since W_m is invariant under $\mathrm{Aut}\, W_n$, the semi-direct product is well-defined.

Proposition 11.1. *Let $n \geq 0$. There is an injective group homomorphism*

$$\rho_n : \mathrm{Gal}(k(\alpha_n, \omega_n)/k) \longrightarrow \mathrm{Aut}\, W_n \ltimes W_n$$

Proof. Let $\sigma \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k)$. Let ε_σ be the restriction of σ to W_n, and let $\omega_\sigma = \sigma(\alpha_n) \dot{-} \alpha_n$. Define $\rho_n(\sigma) = (\varepsilon_\sigma, \omega_\sigma)$.

It is well known that $\varepsilon_\sigma \in \mathrm{Aut}\, W_n$. Moreover, by lemma 10.3, $\omega_\sigma \in W_n$, therefore $\rho_n(\sigma) = (\varepsilon_\sigma, \omega_\sigma) \in \mathrm{Aut}\, W_n \ltimes W_n$.

Let σ, τ be two automorphisms of $k(\alpha_n, \omega_n)/k$. Then

$$\varepsilon_{\sigma\tau} = (\sigma\tau) \restriction_{W_n} = \varepsilon_\sigma \varepsilon_\tau$$

and

$$\begin{aligned}\sigma\tau(\alpha_n) \dot{-} \alpha_n = \sigma\tau(\alpha_n) \dot{-} \sigma(\alpha_n) \dotplus \sigma(\alpha_n) \dot{-} \alpha_n = \\ \sigma(\tau(\alpha_n) \dot{-} \alpha_n) \dotplus (\sigma(\alpha_n) \dot{-} \alpha_n) = \varepsilon_\sigma(\omega_\tau) \dotplus \omega_\sigma \quad (11.1)\end{aligned}$$

hence $\rho_n(\sigma\tau) = \rho_n(\sigma)\rho_n(\tau)$.

Assume that $\varepsilon_\sigma = 1$ and $\omega_\sigma = 0$. Then $\sigma(\omega_n) = \omega_n$ and $\sigma(\alpha_n) = \alpha_n$, thus σ is the identity on $k(\alpha_n, \omega_n)$. Hence ρ_n is injective. $\square$

We will now determine the image of ρ_n. In order to do that, we need a general lemma on Galois groups.

Let L/F be a finite Galois extension of fields. Let $F \subseteq K \subseteq L$ be intermediate field and assume that K/F is also Galois. Write $G = \mathrm{Gal}(L/F)$, $H = \mathrm{Gal}(L/K)$, $\Delta = \mathrm{Gal}(K/F)$, and assume that H is *abelian*. We will use additive notation when referring to the group H.

Let $\sigma \in H$, and $\delta \in \Delta$. Let $\tilde{\delta}$ be an extension of δ to L/F. Define

$$\langle \delta, \sigma \rangle = \tilde{\delta}\sigma\tilde{\delta}^{-1} \quad (11.2)$$

Lemma 11.2. *The pairing defined in* (11.2) *satisfies the following properties:*

1. $\langle \delta, \sigma \rangle \in H$
2. *The definition in* (11.2) *does not depend on the particular choice of an extension* $\tilde{\delta}$ *of* δ.
3. $\langle \delta, \sigma_1 + \sigma_2 \rangle = \langle \delta, \sigma_1 \rangle + \langle \delta, \sigma_2 \rangle$
4. $\langle \delta_1 \delta_2, \sigma \rangle = \langle \delta_1, \langle \delta_2, \sigma \rangle \rangle$

Proof. Let $\sigma \in H$, $\delta \in \Delta$, and choose an extension $\tilde{\delta}$ of δ to L/F.

1. Let $x \in K$. Then, since σ fixes K pointwise,

$$\tilde{\delta}\sigma\tilde{\delta}^{-1}(x) = \delta(\delta^{-1}(x)) = x$$

thus $\langle \delta, \sigma \rangle \in H$.

2. Let δ_1, δ_2 be two extensions of δ. As $\delta_1(x) = \delta_2(x) = \delta(x)$ for every $x \in K$, we have $\delta_2\delta_1^{-1} \in H$.

We already know that $\delta_1\sigma\delta_1^{-1} \in H$. Since H is abelian, the elements $\delta_2\delta_1^{-1}$ and $\delta_1\sigma\delta_1^{-1}$ commute. Therefore,

$$\delta_2\sigma\delta_2^{-1} = (\delta_2\delta_1^{-1})(\delta_1\sigma\delta_1^{-1})(\delta_2\delta_1^{-1})^{-1} = \delta_1\sigma\delta_1^{-1}$$

and $\langle \delta, \sigma \rangle$ does not depend on the particular choice of an extension of δ.

3. This is clear, as

$$\tilde{\delta}\sigma_1\sigma_2\tilde{\delta}^{-1} = (\tilde{\delta}\sigma_1\tilde{\delta}^{-1})(\tilde{\delta}\sigma_2\tilde{\delta}^{-1})$$

4. If $\tilde{\delta_1}$ and $\tilde{\delta_2}$ are extensions of δ_1,δ_2 resp., then $\tilde{\delta_1}\tilde{\delta_2}$ is an extension of $\delta_1\delta_2$, and the result is clear from the definition (and the independence on the extension).

□

In our setting, $G = \mathrm{Gal}(k(\alpha_n, \omega_n)/k)$, $H = \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$ and $\Delta = \mathrm{Gal}(k(\omega_n)/k)$.

Lemma 11.3. *The extension* $k(\alpha_n, \omega_n)/k(\omega_n)$ *is abelian.*

Proof. Let $\sigma \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$ and consider ω_σ defined in the proof of proposition 11.1.

Let $\sigma, \tau \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$. By (11.1),

$$\omega_{\sigma\tau} = \sigma(\omega_\tau) \dot{+} \omega_\sigma$$

but since σ acts trivially on W_n, we actually have

$$\omega_{\sigma\tau} = \omega_\tau \dot{+} \omega_\sigma$$

hence the mapping $\sigma \mapsto \omega_\sigma$ is a homomorphism. It is injective, since if $\omega_\sigma = 0$, then $\sigma(\alpha_n) = \alpha_n$ and σ is the identity on $k(\alpha_n, \omega_n)$.

Now the lemma follows, as $\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$ is embedded in the abelian group W_n. □

We will now use the pairing defined in (11.2). First, we connect this pairing to ρ_n.

Lemma 11.4. *Let $\sigma \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$, $\delta \in \mathrm{Gal}(k(\omega_n)/k)$. Then*

$$\omega_{\langle \delta, \sigma \rangle} = \delta(\omega_\sigma)$$

Proof. Let $\tilde{\delta}$ be an extension of δ to $k(\alpha_n, \omega_n)$. By (11.1)

$$\omega_{\tilde{\delta}\sigma\tilde{\delta}^{-1}} = \tilde{\delta}(\omega_{\sigma\tilde{\delta}^{-1}}) \dot{+} \omega_{\tilde{\delta}} = \tilde{\delta}(\sigma(\omega_{\tilde{\delta}^{-1}}) \dot{+} \omega_\sigma) \dot{+} \omega_{\tilde{\delta}} \tag{11.3}$$

Since σ acts trivially on W_n, we have $\sigma(\omega_{\tilde{\delta}^{-1}}) = \omega_{\tilde{\delta}^{-1}}$. We also have

$$\tilde{\delta}(\omega_{\tilde{\delta}^{-1}}) = \tilde{\delta}(\tilde{\delta}^{-1}(\alpha_n) \dot{-} \alpha_n) = \dot{-}\, \omega_{\tilde{\delta}}$$

Substituting this in (11.3), we get

$$\omega_{\tilde{\delta}\sigma\tilde{\delta}^{-1}} = \tilde{\delta}(\omega_\sigma) = \delta(\omega_\sigma)$$

□

Lemma 11.5. *Let W be a subgroup of the additive group of W_n, and assume also that W is invariant under $\mathrm{Gal}(k(\omega_n)/k)$.*

Then there exists $-1 \leq m \leq n$ such that $W = W_m$.

Proof. By local class field theory, there is a one-to-one correspondence between $\mathrm{Gal}(k(\omega_n)/k)$ and U/U_{n+1}. Thus if $\omega \in W$, then $u \cdot \omega \in W$ for every $u \in U$.

We will show that W is an $\mathfrak{o}$-submodule of W_n. Let $u_1 = 1 + \pi^2$ and $u_2 = 1 + \pi + \pi^2$ be two units, and let $\omega \in W$. Since W is invariant under the Galois group and since it is an additive subgroup, we deduce that

$$\pi \cdot \omega = u_2 \cdot \omega \dot{-} u_1 \cdot \omega \in W$$

and therefore $\langle \pi \rangle \cdot \omega \subseteq W$ (apply the same argument inductively). As $U \cdot \omega \subseteq W$, we conclude that $\mathfrak{o} \cdot \omega \in W$.

Now the result follows from the fact that the only submodules of W_n are W_m for $m \leq n$. □

Lemma 11.6. *There exists $-1 \le m \le n$ for which*

$$\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n)) \cong W_m$$

Proof. In the proof of lemma 11.3 we saw that there is an injection

$$\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n)) \longrightarrow W_n$$

defined by $\sigma \mapsto \omega_\sigma$.

The image of that injection is a subgroup of the additive group of W_n. By lemma 11.4, it is also invariant under every $\delta \in \mathrm{Gal}(k(\omega_n)/k)$. Finally, by lemma 11.5, there exists $-1 \le m \le n$ such that this image equals W_m. □

Definition. A group G is *of type* $\Gamma_{n,m}$ if there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_m & \longrightarrow & G & \longrightarrow & \mathrm{Aut}\, W_n & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & W_n & \xrightarrow{i} & \mathrm{Aut}\, W_n \ltimes W_n & \xrightarrow{p} & \mathrm{Aut}\, W_n & \longrightarrow & 1 \end{array} \tag{11.4}$$

where the middle vertical arrow is an injection, the other vertical arrows are the canonical embeddings, and the horizontal maps i and p are defined by

$$i : \omega \longmapsto (1, \omega)$$
$$p : (\varepsilon, \omega) \longmapsto \varepsilon$$

Groups of type $\Gamma_{n,m}$ can be considered as subgroups of $\mathrm{Aut}\, W_n \ltimes W_n$. A typical element in such group can thus be viewed as a pair (ε, ω) for $\varepsilon \in \mathrm{Aut}\, W_n$ and $\omega \in W_n$. The commutativity of the above diagram implies that elements of the form $(1, \omega)$ belong to a group of type $\Gamma_{n,m}$ if and only if $\omega \in W_m$. It also implies that for every $\varepsilon \in \mathrm{Aut}\, W_n$, there is an $\omega \in W_n$ such that (ε, ω) lies in the group.

Proposition 11.7. *The extension $k(\alpha_n, \omega_n)/k$ is Galois. Its Galois group is of type $\Gamma_{n,m}$, where $-1 \le m \le n$.*

Proof. By proposition 10.4, $k(\alpha_n, \omega_n)/k$ is Galois. Let us compute $\mathrm{Im}\, \rho_n$ for

$$\rho_n : \mathrm{Gal}(k(\alpha_n, \omega_n)/k) \longrightarrow \mathrm{Aut}\, W_n \ltimes W_n$$

defined in proposition 11.1. Since ρ_n is injective, we will get an isomorphism between the Galois group and $\mathrm{Im}\, \rho_n$.

By lemma 11.6, there is an $-1 \le m \le n$ such that the elements of the form $(1, \omega)$ which lie in $\mathrm{Im}\, \rho_n$ are exactly the ones for which $\omega \in W_m$.

The mapping $\delta \mapsto \varepsilon_\delta$ is an isomorphism between $\mathrm{Gal}(k(\omega_n)/k)$ and $\mathrm{Aut}\, W_n$. Since any such δ can be extended to $k(\alpha_n, \omega_n)$, we get that for every $\varepsilon \in \mathrm{Aut}\, W_n$, there is an $\omega(\varepsilon)$ such that $(\varepsilon, \omega(\varepsilon)) \in \mathrm{Im}\, \rho_n$.

Combining these facts, we get a short exact sequence

$$0 \longrightarrow W_m \xrightarrow{\ i'\ } \operatorname{Im}\rho_n \xrightarrow{\ p'\ } \operatorname{Aut} W_n \longrightarrow 1$$

with respect to the maps

$$i' : \omega \longmapsto (1, \omega)$$
$$p' : (\varepsilon, \omega) \longmapsto \varepsilon$$

As $\operatorname{Im}\rho_n$ is a subgroup of $\operatorname{Aut} W_n \ltimes W_n$, it is easy to see that the diagram in (11.4) commutes. $\square$

The value of m depends on the choice of a in the construction of the fields $k(\alpha_n, \omega_n)$. The remainder of this section is devoted to the understanding of this dependency.

Let $\mathfrak{p}_n$ be the maximal ideal of $k(\omega_n)$. Denote by $\pi^i \cdot \mathfrak{p}_n$ the set

$$\pi^i \cdot \mathfrak{p}_n = \left\{ \pi^i \cdot x : x \in \mathfrak{p}_n \right\}$$

for $i \geq 0$. Since $\mathfrak{p}_n$ is topologically closed, the sets $\pi^i \cdot \mathfrak{p}_n$ are also closed and contained in $\mathfrak{p}_n$.

Lemma 11.8. $k \cap \pi^{n+1} \cdot \mathfrak{p}_n \subseteq \mathfrak{p}^2$.

Proof. Let $\beta \in \mathfrak{p}_n$. Recall that $[\pi^{n+1}] \in X\mathfrak{o}[[X]]$, and by the proof of lemma 10.2,

$$[\pi^{n+1}](X) \equiv X^{q^{n+1}} \pmod{\mathfrak{p}}$$

Therefore, $\pi^{n+1} \cdot \beta = \pi\gamma + \beta^{q^{n+1}}$ where $\gamma \in \mathfrak{p}_n$.

Since $k(\omega_n)/k$ is totally ramified of degree $(q-1)q^n$, we have $\mu(\beta) \geq 1/(q-1)q^n$ (recall that μ is an extension of the valuation ν to the algebraic closure Ω).

Now, as $\mu(\gamma) > 0$, we get $\mu(\pi\gamma) > 1$. We also have

$$\mu(\beta^{q^{n+1}}) \geq \frac{q^{n+1}}{(q-1)q^n} > 1 \quad .$$

It follows that $\mu(\pi^{n+1} \cdot \beta) > 1$. In particular, if $\pi^{n+1} \cdot \beta \in k$, then its valuation is at least 2, and it is contained in $\mathfrak{p}^2$. $\square$

Proposition 11.9. *Let m be the integer for which*

$$a \in \pi^{n-m} \cdot \mathfrak{p}_n \setminus \pi^{n-m+1} \cdot \mathfrak{p}_n \quad .$$

Then $0 \leq m \leq n$, and $\operatorname{Gal}(k(\alpha_n, \omega_n)/k)$ is of type $\Gamma_{n,m}$.

Proof. Since $\pi^0 \cdot \mathfrak{p}_n = \mathfrak{p}_n$, we have a disjoint union decomposition

$$\mathfrak{p} = \bigcup_{i=0}^{\infty} \left(k \cap \left(\pi^i \cdot \mathfrak{p}_n \setminus \pi^{i+1} \cdot \mathfrak{p}_n\right)\right)$$

But by the lemma, $\pi^{n+1} \cdot \mathfrak{p}_n \subseteq \mathfrak{p}^2$, hence

$$\mathfrak{p} \setminus \mathfrak{p}^2 \subseteq \bigcup_{i=0}^{n} \left(k \cap \left(\pi^i \cdot \mathfrak{p}_n \setminus \pi^{i+1} \cdot \mathfrak{p}_n\right)\right)$$

It follows that if a is a prime of k, then m defined as above satisfies $0 \leq m \leq n$.

First, assume that $\mathrm{Gal}(k(\alpha_n, \omega_n)/k)$ is of type $\Gamma_{n,m}$ (proposition 11.7 ensures that this is the form of the Galois group). Then $\omega_\sigma \in W_m$ for every automorphism $\sigma \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$. Thus

$$\pi^{m+1} \cdot (\sigma(\alpha_n) \dot{-} \alpha_n) = 0$$

for every such σ, or equivalently, since σ commutes with $[\pi^{m+1}] \in \mathfrak{o}[[X]]$,

$$\sigma(\pi^{m+1} \cdot \alpha_n) = \pi^{m+1} \cdot \alpha_n$$

thus $\pi^{m+1} \cdot \alpha_n \in k(\omega_n)$.

By lemma 10.2, $k(\alpha_n)/k$ is a totally ramified extension of degree q^{n+1} and α_n is a prime in that extension. In particular, $\alpha_n \in \mathfrak{p}_{\bar{\Omega}}$, and $\pi^{m+1} \cdot \alpha_n \in \mathfrak{p}_{\bar{\Omega}}$. Therefore $\pi^{m+1} \cdot \alpha_n \in \mathfrak{p}_n$, and

$$a = \pi^{n+1} \cdot \alpha_n = \pi^{n-m} \cdot (\pi^{m+1} \cdot \alpha_n) \in \pi^{n-m} \cdot \mathfrak{p}_n$$

For the opposite direction, assume that $a = \pi^{n-m} \cdot \beta$ for $\beta \in \mathfrak{p}_n$. Then

$$\pi^{n+1} \cdot \alpha_n = \pi^{n-m} \cdot (\pi^{m+1} \cdot \alpha_n) = a = \pi^{n-m} \cdot \beta$$

hence $\beta \dot{-} \pi^{m+1}\alpha_n \in W_{n-m-1}$. Since $\beta \in \mathfrak{p}_n$ and $W_{n-m-1} \subseteq W_n \subseteq \mathfrak{p}_n$, we have

$$\pi^{m+1}\alpha_n \in \mathfrak{p}_n$$

Thus for every $\sigma \in \mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$,

$$\sigma(\pi^{m+1} \cdot \alpha_n) = \pi^{m+1} \cdot \alpha_n$$

Again, since σ commutes with $[\pi^{m+1}] \in \mathfrak{o}[[X]]$, this is equivalent to

$$\pi^{m+1} \cdot \omega_\sigma = \pi^{m+1}(\sigma(\alpha_n) \dot{-} \alpha_n) = 0$$

Therefore $\omega_\sigma \in W_m$ for every such σ.

The proposition now follows from the combination of the above arguments and the special form of the Galois group; this group is of type $\Gamma_{n,m'}$ where m' is characterized by the fact that

$$\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n)) \cong W_{m'}$$

Assume that $a \in \pi^{n-m} \cdot \mathfrak{p}_n \setminus \pi^{n-m+1} \cdot \mathfrak{p}_n$. The second argument above implies that the image of the subgroup $\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n))$ is contained in W_m, hence $m' \leq m$. But the first argument implies that if the Galois group is of type $\Gamma_{n,m'}$, then $a \in \pi^{n-m'} \cdot \mathfrak{p}_n$, hence we must have $m = m'$. $\square$

12 Central Series of $\mathrm{Gal}(k(\alpha_n, \omega_n)/k)$

The groups $\mathrm{Gal}(k(\alpha_n, \omega_n)/k)$ are of type $\Gamma_{n,m}$ for $0 \leq m \leq n$. We will now compute the upper and lower central series of these groups. The nature of the results we shall obtain depends on the value of q, the order of the residue field of k. It seems appropriate to distinguish between two cases: the case where $q > 2$ and the case where $q = 2$.

The case $q > 2$

Let G be of type $\Gamma_{n,m}$ where $n \geq 0$ and $0 \leq m \leq n$ (in the case where $m = -1$ we have merely $G = \mathrm{Aut}\, W_n \cong U/U_{n+1}$ which is an abelian group and the upper (lower) series are trivial).

Lemma 12.1. *Let $\omega \in W_m$, and assume that $\varepsilon(\omega) = \omega$ for every $\varepsilon \in \mathrm{Aut}\, W_m$. Then $\omega = 0$.*

Proof. There is an isomorphism $\mathrm{Aut}\, W_m \cong \mathrm{Gal}(k(\omega_m)/k)$ defined by $\sigma \mapsto \varepsilon_\sigma$ (the restriction of σ to W_m). Thus the condition in the lemma can be reformulated as $\sigma(\omega) = \omega$ for every $\sigma \in \mathrm{Gal}(k(\omega_m)/k)$. Therefore, $\omega \in k \cap W_m$.

If ω generates the module W_i $(i \geq 0)$, then it is well known that $k(\omega) = k(W_i)$, an extension of degree $(q-1)q^i > 1$ over k. It follows that ω generates $W_{-1} = 0$, i.e. $\omega = 0$. (Note that the assumption $q > 2$ is necessary for this implication to hold). $\square$

Lemma 12.2. *Let G be of type $\Gamma_{n,m}$. Then*

(i) $\mathrm{Z}(G) \subseteq \Big\{(\varepsilon, \omega) : \ \varepsilon \text{ acts trivially on } W_m\Big\}$

(ii) If $(1, \omega) \in \mathrm{Z}(G)$, *then* $\omega = 0$.

Proof. Let $(\varepsilon, \omega) \in \mathrm{Z}(G)$. For every $(\varepsilon', \omega') \in G$, we have

$$(\varepsilon, \omega)(\varepsilon', \omega') = (\varepsilon', \omega')(\varepsilon, \omega)$$

Carrying out the multiplication, we get the constraints:

$$\begin{aligned} \varepsilon\varepsilon' &= \varepsilon'\varepsilon \\ \omega \dotplus \varepsilon(\omega') &= \omega' \dotplus \varepsilon'(\omega) \end{aligned} \tag{12.1}$$

where the first constraint is always satisfied, as $\operatorname{Aut} W_n$ is an abelian group.

Take $\varepsilon' = 1$ and $\omega' \in W_m$ arbitrary. Substituting in (12.1), we see that

$$\varepsilon(\omega') = \omega'$$

hence ε acts trivially on W_m.

For the second claim, assume that $(1, \omega) \in \mathrm{Z}(G)$. Then by (12.1),

$$\omega = \varepsilon'(\omega) \tag{12.2}$$

for every $(\varepsilon', \omega') \in G$. Since the projection from G to $\operatorname{Aut} W_n$ is surjective, we can take in (12.2) any $\varepsilon' \in \operatorname{Aut} W_n$, and deduce, by lemma 12.1, that $\omega = 0$. $\square$

Lemma 12.3. *Let G be of type $\Gamma_{n,m}$ as before. Then*

$$G' = \left\{(1, \omega) : \omega \in W_m\right\} \cong W_m$$

Proof. Consider a commutator $[(\varepsilon, \omega), (\varepsilon', \omega')]$. Its first coordinate equals $[\varepsilon, \varepsilon'] = 1$, since $\operatorname{Aut} W_n$ is abelian. Therefore,

$$G' \subseteq \left\{(1, \omega) : \omega \in W_m\right\}$$

To prove the opposite inclusion, note that the group $\left\{(1, \omega) \in G\right\}$ is normal in G. This follows from the fact that this group is the kernel of the homomorphism $G \to \operatorname{Aut} W_n$ defined by $(\varepsilon, \omega) \mapsto \varepsilon$. The image of this homomorphism is the abelian group $\operatorname{Aut} W_n$, hence we get that

$$\left\{(1, \omega) \in G\right\} \subseteq G'$$

$\square$

Remark. In the proof of this lemma we did not use the assumption $q > 2$. Hence it is also true for $q = 2$.

Lemma 12.4. $\mathrm{Z}_2(G) = \mathrm{Z}(G)$

Proof. Let $z \in \mathrm{Z}_2(G)$. By proposition 8.1, $[z, g] \in G' \cap \mathrm{Z}(G)$ for every $g \in G$. Applying this to our case, using the previous lemmas, we see that if $[z, g] = (\varepsilon, \omega)$, then since $[z, g] \in G'$ we must have $\varepsilon = 1$, and as $[z, g] \in \mathrm{Z}(G)$, we must have $\omega = 0$. Hence $[z, g] = 1$ for every $g \in G$, and therefore $z \in \mathrm{Z}(G)$. $\square$

Corollary. *The upper central series of G gets fixed after the second stage.*

Proof. This is clear from $\mathrm{Z}_2(G) = \mathrm{Z}(G)$. □

We prove symmetrical result for the lower central series.

Lemma 12.5. $G^2 = G^1$

Proof. Let $(1, \omega) \in G^1$, $(\varepsilon', \omega') \in G$. Then

$$[(\varepsilon', \omega'), (1, \omega)] = (1, \varepsilon'(\omega) \dot{-} \omega)$$

Denote by W the subgroup

$$W = \left\langle \varepsilon(\omega) \dot{-} \omega : \varepsilon \in \operatorname{Aut} W_n, \omega \in W_m \right\rangle$$

Let $\varepsilon \in \operatorname{Aut} W_n$. There is $u_\varepsilon \in U$ such that $\varepsilon(\omega) = u_\varepsilon \cdot \omega$ for every $\omega \in W_n$. Thus

$$W = \langle (u-1) \cdot \omega : u \in U, \omega \in W_m \rangle$$

Since $q > 2$, we can find a unit $u \in U \setminus U_1$ for which $u - 1 \in U$. It follows that $[u-1]$ acts on W_m as a permutation, thus $(u-1) \cdot W_m = W_m$ and the lemma follows. □

Proposition 12.6. *Let G be of type $\Gamma_{n,m}$, $n \geq m \geq 0$. Then G is metabelian and non-nilpotent.*

Proof. Consider the normal subgroup G'. Since $G' \cong W_m$, we get that both G' and G/G' are abelian, hence G is metabelian.

If G were nilpotent, then we would have $\mathrm{Z}_n(G) = G$ for some $n \geq 1$. However, we already know that $\mathrm{Z}_n(G) = \mathrm{Z}(G)$ for every $n \geq 1$. As G is non-abelian ($G' \neq 1$), we have $\mathrm{Z}_n(G) = \mathrm{Z}(G) \neq G$, a contradiction. □

Corollary. *Let $n \geq 0$. The extensions $k(\alpha_n, \omega_n)/k$ are metabelian and non-nilpotent. The maximal abelian extension over k contained in $k(\alpha_n, \omega_n)$ equals $k(\omega_n)$.*

Proof. Since $G = \mathrm{Gal}(k(\alpha_n, \omega_n)/k)$ is of type $\Gamma_{n,m}$ for $0 \leq m \leq n$, the first claim follows immediately from the previous proposition. Moreover, since

$$\mathrm{Gal}(k(\alpha_n, \omega_n)/k(\omega_n)) \cong \left\{ (1, \omega) : \omega \in W_m \right\} = G'$$

we get that $\mathrm{Gal}(k(\omega_n)/k)$ is the maximal abelian quotient of G and the second claim follows. □

We now state some consequences of the proposition related to the maximal abelian extensions of some fields.

Notation. Denote by k_π^0 the extension $k(\omega_0)$, where ω_0 is a generator of the module W_0.

Note that the extension k_π^0 depends only on π, and not on the particular choice of the Lubin-Tate series $h(X)$.

Theorem 12.7. *Let K/k be a non-ramified extension. Then the extension $(Kk_\pi^0)^{ab}/K$ is not pro-nilpotent.*

Proof. Let $h(X) \in \mathfrak{o}[[X]]$ a Lubin-Tate power series over k with respect to π, which is also a polynomial of degree q.

Consider the extension $K(\alpha_0, \omega_0)/K$. By proposition 10.5, the extension $k(\alpha_0, \omega_0)/k$ is totally ramified, therefore

$$\mathrm{Gal}(K(\alpha_0, \omega_0)/K) \cong \mathrm{Gal}(k(\alpha_0, \omega_0)/k)$$

is of type $\Gamma_{0,0}$.

We deduce that $K(\alpha_0, \omega_0)/K$ is a finite extension, which is abelian over $K(\omega_0) = Kk_\pi^0$, by lemma 11.3, and not nilpotent, by proposition 12.6.

Since this extension is finite and is contained in $(Kk_\pi^0)^{ab}$, we get that $(Kk_\pi^0)^{ab}/K$ is not pro-nilpotent. ☐

Corollary. *Let K/k be a non-ramified extension.*

Then the extensions $(Kk_\pi)^{ab}/K$ and $(k^{ab})^{ab}/K$ are not pro-nilpotent.

Proof. These extensions contain the extension $(Kk_\pi^0)^{ab}/K$. ☐

The case $q = 2$

Again, let G be of type $\Gamma_{n,m}$ for $n \geq m \geq 0$. The order of G equals $(q-1)q^n \cdot q^{m+1}$ which is a power of 2 (since $q = 2$). In particular, G is a finite p-group ($p = 2$), and therefore nilpotent. The following proposition is an immediate consequence of the nilpotency of G.

Proposition 12.8. *Assume that $q = 2$, and let $n \geq 0$. Then the extensions $k(\alpha_n, \omega_n)/k$ are metabelian and nilpotent.*

Proof. For the proof that these extensions are metabelian, cf. the proof of proposition 12.6. The nilpotency follows from the nilpotency of the groups of type $\Gamma_{n,m}$ in this case. ☐

We will now compute the lower central series. As a consequence, we will determine the nilpotency class of the group G.

Proposition 12.9. *Let G be as before, and let $i \geq 1$. Then the i-th group of the lower central series of G equals*

$$G^i = \left\{ (1, \omega) : \omega \in W_{m+1-i} \right\}$$

In particular, $G^{m+2} = 1$ and G is of nilpotency class $m+2$.

Proof. By lemma 12.3, the proposition is true for $i = 1$. We continue by induction on i; we assume that the proposition is true for i and prove it for $i + 1$.

Let $(1, \omega) \in G^i$, $(\varepsilon', \omega') \in G$. Then

$$[(\varepsilon', \omega'), (1, \omega)] = (1, \varepsilon'(\omega) \dot{-} \omega)$$

and by the induction hypothesis, $\omega \in W_{m+1-i}$.

To determine the image of $\varepsilon(\omega) \dot{-} \omega$ for $\omega \in W_{m+1-i}$, we use an argument similar to the one in the proof of lemma 12.5. Write $\varepsilon(\omega)$ as $u \cdot \omega$ for $u \in U$. Since $q = 2$, we have $U = U_1$ and therefore $u - 1 \in \mathfrak{p}$ for every $u \in U$. It follows that

$$u \cdot \omega \dot{-} \omega = (u - 1) \cdot \omega \in \mathfrak{p} \cdot \omega$$

and we deduce that this subgroup is contained in $\mathfrak{p} \cdot W_{m+1-i} = W_{m-i}$.

Take now $u = 1 + \pi$. As ω runs over W_{m+1-i}, $(u - 1) \cdot \omega$ runs over all elements of W_{m-i}, and the induction step is complete.

Since $W_0 \neq W_{-1} = 0$, we get that $G^{m+1} \neq 1$, $G^{m+2} = 1$. Hence G's nilpotency class equals $m + 2$. □

Part IV
Lower Central Series

13 The Groups $B_{d,\alpha}(H)$

As before, let (k,ν) be a local field, with residue field $\mathbb{F}_q = \mathfrak{o}/\mathfrak{p}$ and prime element π, and let $h(X) \in \mathfrak{o}[[X]]$ be a Lubin-Tate power series with respect to π. Throughout this section, we fix $d \geq 1$.

Let $H \leq U$ be a closed subgroup of U. We define, by transfinite induction, a sequence of subgroups of $\mathbb{F}_{q^d}[[X]]^\times$.

Definition. The groups $B_{d,\alpha}(H)$ are defined as follows:

1. For $\alpha = 1$, define
$$B_{d,1}(H) = \mathbb{F}_{q^d}[[X]]^\times$$
2. For every ordinal α, define
$$B_{d,\alpha+1}(H) = \left\langle \frac{\xi \circ \{u\}}{\xi} : \xi \in B_{d,\alpha}, u \in H \right\rangle$$
where by $\langle A \rangle$ we mean the closure of the subgroup generated by the set A.
3. If α is a limit ordinal (not a successor), define
$$B_{d,\alpha}(H) = \bigcap_{\beta<\alpha} B_{d,\beta}(H)$$

Lemma 13.1. *The groups $B_{d,\alpha}(H)$ satisfy the following properties:*

(i) $B_{d,\alpha}(H_1) \subseteq B_{d,\alpha}(H_2)$ *for* $H_1 \leq H_2$.

(ii) If $u \in U$ *and* $\xi \in B_{d,\alpha}(H)$, *then* $\xi \circ \{u\} \in B_{d,\alpha}(H)$.

(iii) $B_{d,\beta}(H) \subseteq B_{d,\alpha}(H)$ *for* $\alpha < \beta$.

Proof. (i) This is clear for $\alpha = 1$. We proceed by transfinite induction. For successors $\alpha + 1$, since $B_{d,\alpha}(H_1) \subseteq B_{d,\alpha}(H_2)$ by the induction hypothesis and $H_1 \leq H_2$, we get that the set of topological generators of $B_{d,\alpha+1}(H_1)$ is contained in the set of topological generators of $B_{\alpha+1}(H_2)$, thus $B_{d,\alpha+1}(H_1) \subseteq B_{d,\alpha+1}(H_2)$.

For limit ordinals α the induction step is clear, as $B_{d,\alpha}(H)$ is defined as the intersection of all previous $B_{d,\beta}(H)$.

(ii) Again, this is proved by transfinite induction. The statement is clear for $\alpha = 1$, since $B_{d,1}(H) = \mathbb{F}_{q^d}[[X]]^\times$.

Assume the statement is true for an ordinal α. To prove it for $\alpha + 1$, we first note that since the mapping $\eta \mapsto \eta \circ \{u\}$ is a continuous multiplicative endomorphism of $\mathbb{F}_{q^d}[[X]]^\times$, it suffices to show that $\eta \circ \{u\} \in B_{d,\alpha+1}(H)$ for a generator η of $B_{d,\alpha+1}(H)$ and $u \in U$.

Take such a generator η, and write it as $\eta = (\xi \circ \{v\})/\xi$ for $v \in H$, $\xi \in B_{d,\alpha}(H)$. Then

$$\eta \circ \{u\} = \frac{\xi \circ \{v\} \circ \{u\}}{\xi \circ \{u\}} = \frac{(\xi \circ \{u\}) \circ \{v\}}{\xi \circ \{u\}}$$

which is another generator of $B_{d,\alpha+1}(H)$ since $\xi \circ \{u\} \in B_{d,\alpha}(H)$ by the induction hypothesis.

The induction step for limit ordinals α is obvious; if $\xi \in B_{d,\alpha}(H)$, then for every $\beta < \alpha$ we have $\xi \in B_{d,\beta}(H)$, thus by our hypothesis, $\xi \circ \{u\} \in B_{d,\beta}(H)$ for every $u \in U$, hence $\xi \circ \{u\} \in B_{d,\alpha}(H)$ for every $u \in U$.

(iii) It is enough to show $B_{d,\alpha+1}(H) \subseteq B_{d,\alpha}(H)$. Again, we may limit our attention to generators of $B_{d,\alpha+1}$. Such a generator has the form

$$\frac{\xi \circ \{u\}}{\xi}$$

for $\xi \in B_{d,\alpha}(H)$, $u \in H$. This quotient lies in $B_{d,\alpha}(H)$ since $\xi \circ \{u\} \in B_{d,\alpha}(H)$ by the previous statement.

$\square$

We shall now show that we may consider only ordinals $\alpha \leq \omega$. First, a lemma on compact groups.

Lemma 13.2. *Let G be a commutative compact group, and A be a closed subgroup. Let $\{B_n\}_{n\geq 1}$ a decreasing sequence of closed subgroups (that is, $B_n \subseteq B_m$ if $n > m$).*

Then

$$A\left(\bigcap_{n\geq 1} B_n\right) = \bigcap_{n\geq 1} AB_n$$

Proof. Denote by B the intersection of all B_n-s. The inclusion $\subseteq$ is trivial, as $B \subseteq B_n$ for every $n \geq 1$.

To prove the reverse inclusion, let $x \in \bigcap_{n\geq 1} AB_n$. For every $n \geq 1$, write x as $x = a_n b_n$ for $a_n \in A$, $b_n \in B_n$. Since G is compact, we can find a subsequence $\{n_l\}_{l\geq 1}$ such that the two sequences a_{n_l} and b_{n_l} converge.

Write $a = \lim_{l\to\infty} a_{n_l}$, $b = \lim_{l\to\infty} b_{n_l}$. As A is closed, we get that $a \in A$, as a limit of points in A. Since B_{n_l} contains B_n for $n \geq n_l$, we see that all but finite number of elements of the sequence $\{b_{n_l}\}$ belong to B_{n_l}, hence $b \in B_{n_l}$. As this is true for every $l \geq 1$, we obtain $b \in B$.

Now, $ab = \lim_{l\to\infty} a_{n_l} b_{n_l} = x$, hence $x \in AB$, as required. □

Proposition 13.3. *Let $H \leq U$. Then $B_{d,\omega+1}(H) = B_{d,\omega}(H)$.*

Proof. For $r \geq 1$, denote by I_r the subgroup $1 + X^r \mathbb{F}_{q^d}[[X]]$ of $\mathbb{F}_{q^d}[[X]]^\times$. The sequence $\{I_r\}_{r\geq 1}$ forms a filtration of $\mathbb{F}_{q^d}[[X]]^\times$.

The quotient $\mathbb{F}_{q^d}[[X]]^\times / I_r$ is nothing but the multiplicative group of the ring $\mathbb{F}_{q^d}[X]/(X^r)$. In particular, as $\mathbb{F}_{q^d}$ is a finite field, this group is *finite*.

Fix $r \geq 1$ and consider the subgroups $B_{d,\alpha}(H)I_r/I_r$. They form a decreasing sequence of subgroups of the finite group $\mathbb{F}_{q^d}[[X]]^\times/I_r$. Therefore there is an integer $l_r \geq 1$ for which $B_{d,l_r}(H)I_r/I_r = B_{d,l_r+1}(H)I_r/I_r$. It follows that for every ordinal $\alpha \geq l_r$,

$$B_{d,\alpha}(H)I_r = B_{d,l_r}(H)I_r$$

and in particular, $B_{d,\omega+1}(H)I_r = B_{d,\omega}(H)I_r$ (since both subgroups equal $B_{d,l_r}(H)$).

We deduce that $B_{d,\omega}(H) \subseteq B_{d,\omega+1}(H)I_r$ for every $r \geq 1$. Therefore

$$B_{d,\omega}(H) \subseteq \bigcap_{r\geq 1} B_{d,\omega+1}(H)I_r = B_{d,\omega+1}(H)$$

where the last equality follows from lemma 13.2 and $\cap_{r\geq 1} I_r = 1$.

As the reverse inclusion is obvious, the proposition follows. □

The next result connects the group $B_{d,\alpha}(H_1H_2)$, for two subgroups H_1, H_2 of U, with the groups associated with H_1 and H_2.

Lemma 13.4. *Let H_1, H_2 be subgroups of U. Then for every $\alpha \leq \omega$,*

$$B_{d,\alpha}(H_1H_2)B_{d,2}(H_2) = B_{d,\alpha}(H_1)B_{d,2}(H_2)$$

Proof. As $H_1H_2 \geq H_2$, the inclusion $\supseteq$ is clear. To prove the reverse inclusion, it is enough to show that $B_{d,\alpha}(H_1H_2) \subseteq B_{d,\alpha}(H_1)B_{d,2}(H_2)$.

Again, we use (transfinite) induction. The statement is clear for $\alpha = 1$, as both sides equal $\mathbb{F}_{q^d}[[X]]^\times$. Assume now that it is true for an ordinal α, and take a generator η of $B_{d,\alpha+1}(H_1H_2)$. Write η as

$$\eta = \frac{\xi \circ \{u\}}{\xi} \tag{13.1}$$

for $\xi \in B_{d,\alpha}(H_1H_2)$ and $u \in H_1H_2$.

Write $u = u_1 u_2$ with $u_1 \in H_1$, $u_2 \in H_2$. By the induction hypothesis, we can write $\xi = \xi_1 \xi_2$ for $\xi_1 \in B_{d,\alpha}(H_1)$, $\xi_2 \in B_{d,2}(H_2)$. We can therefore rewrite (13.1) as

$$\begin{aligned} \eta = \frac{(\xi_1\xi_2) \circ \{u\}}{\xi_1\xi_2} &= \frac{\xi_1 \circ \{u_1 u_2\}}{\xi_1} \cdot \frac{\xi_2 \circ \{u\}}{\xi_2} = \\ &= \frac{(\xi_1 \circ \{u_2\}) \circ \{u_1\}}{\xi_1 \circ \{u_2\}} \cdot \frac{\xi_1 \circ \{u_2\}}{\xi_1} \cdot \frac{\xi_2 \circ \{u\}}{\xi_2} \end{aligned} \tag{13.2}$$

Now, as $\xi_1 \in B_{d,\alpha}(H_1)$, we get that $\xi_1 \circ \{u_2\} \in B_{d,\alpha}(H_1)$ and therefore the leftmost element in the product belongs to $B_{d,\alpha+1}(H_1)$. Since $\xi_1 \in \mathbb{F}_{q^d}[[X]]^\times$ and $u_2 \in H_2$, it follows that the middle element belongs to $B_{d,2}(H_2)$. Finally, since $\xi_2 \in B_{d,2}(H_2)$ and $u \in U$, we get by lemma 13.1 that the rightmost element also belongs to $B_{d,2}(H_2)$, and η lies in $B_{d,\alpha+1}(H_1)B_{d,2}(H_2)$

If $\alpha = \omega$ is a limit ordinal, then by the induction hypothesis and lemma 13.2 for the compact group $\mathbb{F}_{q^d}[[X]]^\times$,

$$\begin{aligned} B_{d,\alpha}(H_1H_2) = \bigcap_{\beta<\alpha} B_{d,\beta}(H_1H_2) \subseteq \bigcap_{\beta<\alpha} B_{d,\beta}(H_1)B_{d,2}(H_2) = \\ \left(\bigcap_{\beta<\alpha} B_{d,\beta}(H_1)\right) B_{d,2}(H_2) = B_{d,\alpha}(H_1)B_{d,2}(H_2) \end{aligned}$$

□

Proposition 13.5. *Let H_1,H_2 be subgroups of U. Then*

$$B_{d,\omega}(H_1H_2) = B_{d,\omega}(H_1)B_{d,\omega}(H_2)$$

Proof. First, note that the inclusion $\supseteq$ follows from the fact that $H_1H_2 \geq H_1$, $H_1H_2 \geq H_2$; the group on the LHS contains both groups in the RHS, thus it contains their product. It remains to show the opposite inclusion.

We start by proving that for every $n, m \geq 2$,

$$\begin{aligned} B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1) \cdot B_{d,\omega}(H_2) \cdot (B_{d,m}(H_1) \cap B_{d,n}(H_2)) \\ \cdot (B_{d,2}(H_1) \cap B_{d,n+1}(H_2)) \end{aligned} \tag{13.3}$$

We prove this by double induction; we assume (13.3) for a pair (n, m) and prove it for $(n, m+1)$. Then we prove it for $(n+1, 2)$ assuming it for (n, m) for every $m < \omega$. This double induction is actually ordinary transfinite induction for ordinals smaller than $\omega \cdot \omega$.

First, we prove (13.3) for $n = 2$, $m = 2$. This is merely a double application of lemma 13.4. By this lemma, we get

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,2}(H_2)$$

and by exchanging the roles of H_1, H_2, we also get

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_2)B_{d,2}(H_1)$$

to that

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,2}(H_2) \cap B_{d,\omega}(H_2)B_{d,2}(H_1) \tag{13.4}$$

Assume now that $x \in B_{d,\omega}(H_1)B_{d,2}(H_2) \cap B_{d,\omega}(H_2)B_{d,2}(H_1)$. Then we can write x as

$$x = y_1z_2 = y_2z_1$$

for $y_1 \in B_{d,\omega}(H_1)$, $y_2 \in B_{d,\omega}(H_2)$, $z_1 \in B_{d,2}(H_1)$, $z_2 \in B_{d,2}(H_2)$. Hence

$$B_{d,2}(H_2) \ni \frac{z_2}{y_2} = \frac{z_1}{y_1} \in B_{d,2}(H_1)$$

so that these quotients lie in the intersection of the two groups. Therefore,

$$x = y_1 \cdot y_2 \cdot \frac{z_2}{y_2} \in B_{d,\omega}(H_1)B_{d,\omega}(H_2)\left(B_{d,2}(H_1) \cap B_{d,2}(H_2)\right)$$

Combining this and (13.4), we finally get

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,\omega}(H_2)\left(B_{d,2}(H_1) \cap B_{d,2}(H_2)\right)$$

and (13.3) follows for $n = 2$, $m = 2$.

Assume now that (13.3) is true for (n, m). Since $B_{d,\omega+1}(H) = B_{d,\omega}(H)$ for every H, it is enough to show that elements of the form $\xi \circ \{u\}/\xi$ for $\xi \in B_{d,\omega}(H)$, $u \in H_1H_2$ lie in the RHS of (13.3).

Since $B_{d,\omega}(H_i)$ $(i = 1, 2)$ are closed under composition with $\{u\}$, it is sufficient to show that

$$\frac{\xi \circ \{u\}}{\xi} \in \left(B_{d,m+1}(H_1) \cap B_{d,n}(H_2)\right)\left(B_{d,2}(H_1) \cap B_{d,n+1}(H_2)\right)$$

for $\xi \in \left(B_{d,m}(H_1) \cap B_{d,n}(H_2)\right)\left(B_{d,2}(H_1) \cap B_{d,n+1}(H_2)\right)$.

Write such ξ as $\xi = \xi_1\xi_2$ for $\xi_1 \in B_{d,m}(H_1) \cap B_{d,n}(H_2)$, $\xi_2 \in B_{d,2}(H_1) \cap B_{d,n+1}(H_2)$. Write $u = u_1u_2$ for $u_1 \in H_1$, $u_2 \in H_2$. Then by (13.2),

$$\frac{\xi \circ \{u\}}{\xi} = \frac{(\xi_1 \circ \{u_2\}) \circ \{u_1\}}{\xi_1 \circ \{u_2\}} \cdot \frac{\xi_1 \circ \{u_2\}}{\xi_1} \cdot \frac{\xi_2 \circ \{u\}}{\xi_2}$$

Since $\xi_1 \in B_{d,m}(H_1) \cap B_{d,n}(H_2)$, we get that the leftmost element in the product lies in $B_{d,m+1}(H_1) \cap B_{d,n}(H_2)$ (because $u_1 \in H_1$), the middle element lies in $B_{d,m}(H_1) \cap B_{d,n+1}(H_2)$ (because $u_2 \in H_2$). Similarly, we get that the rightmost element lies in $B_{d,2}(H_1) \cap B_{d,n+1}(H_2)$. Therefore the product lies in

$$(B_{d,m+1}(H_1) \cap B_{d,n}(H_2))\,(B_{d,2}(H_1) \cap B_{d,n+1}(H_2))$$

and (13.3) is also true for $(n, m+1)$.

Assume now that (13.3) is true for all pairs (n, m) where n is fixed and $m < \omega$. Then

$$\begin{aligned} &B_{d,\omega}(H_1H_2) \subseteq \\ &\bigcap_{m \geq 2} B_{d,\omega}(H_1)B_{d,\omega}(H_2)\,(B_{d,m}(H_1) \cap B_{d,n}(H_2))\,(B_{d,2}(H_1) \cap B_{d,n+1}(H_2)) \\ &=B_{d,\omega}(H_1)B_{d,\omega}(H_2)\,(B_{d,\omega}(H_1) \cap B_{d,n}(H_2))\,(B_{d,2}(H_1) \cap B_{d,n+1}(H_2)) \\ &=B_{d,\omega}(H_1)B_{d,\omega}(H_2)\,(B_{d,2}(H_1) \cap B_{d,n+1}(H_2)) \end{aligned}$$

by lemma 13.2, and therefore (13.3) is true for $(n+1, 2)$.

Consider (13.3) for (n, m). Write it as

$$\begin{aligned} B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,\omega}(H_2)\,(B_{d,m}(H_1) \cap B_{d,n}(H_2)) \cdot \\ \cdot (B_{d,2}(H_1) \cap B_{d,n+1}(H_2)) \subseteq B_{d,m}(H_1)B_{d,n+1}(H_2) \end{aligned}$$

By taking the intersection over all m we get

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,n+1}(H_2)$$

for every $n \geq 2$. By taking intersection over all n, we finally get

$$B_{d,\omega}(H_1H_2) \subseteq B_{d,\omega}(H_1)B_{d,\omega}(H_2)$$

as required. $\square$

14 The Extensions $N_{d,\alpha}(H)$

We are now going to make a connection between the subgroups $B_{d,\alpha}(H)$ defined in the last section and maximal (pro-)nilpotent extensions of local fields.

We begin by establishing the necessary background on (pro-)nilpotent extensions, in the following few lemmas.

Lemma 14.1. *Let L/K be an extension with Galois group G. For every $n \geq 1$, let L_n be the extension defined by $\mathrm{Gal}(L/L_n) = G^n$ (recall that G^n is the closed n-th commutator subgroup of G).*

Then the extension L_n/K is the maximal extension over K with nilpotency class n contained in L.

Proof. $\mathrm{Gal}(L_n/K) = G/G^n$. This group is nilpotent of class n, as every $n+1$-th commutator

$$[\dots[[x_1, x_2], x_3]\dots, x_{n+1}] \tag{14.1}$$

is the image of such a commutator in G. Since all such commutators in G lie in G^n, we must have that the commutator in (14.1) equals 1.

Assume that $\mathrm{Gal}(M/K)$ is nilpotent of class n. Then the image of every $n+1$-th commutator in G as in (14.1) modulo $\mathrm{Gal}(L/M)$ is 1, meaning that all such commutators lie in $\mathrm{Gal}(L/M)$. Thus $G^n \subseteq \mathrm{Gal}(L/M)$, and $M \subseteq L_n$. ☐

Lemma 14.2. *Let L/K be as in the previous lemma. Denote by G^ω the intersection of the groups G^n, and by L_ω the union of all fields L_n.*

Then $\mathrm{Gal}(L/L_\omega) = G^\omega$ *and L_ω/K is the maximal pro-nilpotent extension over K contained in L.*

Proof. The groups $\mathrm{Gal}(L_n/K)$ is nilpotent. Since

$$\mathrm{Gal}(L_\omega/K) = \varprojlim \mathrm{Gal}(L_n/K)$$

we get that $\mathrm{Gal}(L_\omega/K)$ is pro-nilpotent.

Let M/K be pro-nilpotent in L. Let $x \in M$, and consider the normal closure of $K(x)/K$. As this is a finite extension in M and M/K is pro-nilpotent, it is nilpotent of some class n, hence $x \in L_n$. It follows that $M \subseteq L_\omega$. ☐

Notation. Let L/k be Galois, $k \subseteq L \subseteq (k_\pi k_d^{nr})^{ab}$, and let $n \geq 1$. Denote by $M_{d,n}(L)$ the maximal extension over L with nilpotency class n contained in $(k_\pi k_d^{nr})^{ab}$.

Denote by $M_{d,\omega}(L)$ the maximal pro-nilpotent extension over L contained in $(k_\pi k_d^{nr})^{ab}$

Remark. By the last lemma, $M_{d,\omega}(L)$ is the union of all $M_{d,n}(L)$ for $n \geq 1$.

As in the last section, we still keep $d \geq 1$ fixed. By metabelian local class field theory, there is an isomorphism $\imath : \mathfrak{G}_d(k, \phi) \xrightarrow{\cong} \mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k)$. There is also an injection $\mathbb{F}_{q^d}[[X]]^\times \longrightarrow \mathfrak{G}_d(k, \phi)$, $\xi \mapsto (1, \xi)$. We denote, for $B \subseteq \mathbb{F}_{q^d}[[X]]^\times$, the image of this injection by $1 \times B$.

Definition. Let α be an ordinal. Define $N_{d,\alpha}(H)$ as the field contained in $(k_\pi k_d^{nr})^{ab}$ for which

$$\mathrm{Gal}((k_\pi k_d^{nr})^{ab}/N_{d,\alpha}(H)) = \imath(1 \times B_{d,\alpha}(H))$$

Remark. Since $B_{d,\omega}(H)$ is the intersection of all $B_{d,n}(H)$, the field $N_{d,\omega}(H)$ is the union of the fields $N_{d,n}(H)$.

The following lemma connects the extensions $M_{d,n}(L)$ and $N_{d,n}(H)$.

Lemma 14.3. *Let $H \leq U$, $P \leq \langle \pi^d \rangle^{\hat{\mathbb{Z}}}$ be closed subgroups. Let L be the field corresponding to the group $P \times H$ by local class field theory (that is, $\mathrm{Gal}(k^{ab}/L) = P \times H$).*

Then

$$N_{d,n}(L) \subseteq M_{d,n}(H) \subseteq N_{d,n+1}(L)$$

Proof. The subgroup $(k_\pi k_d^{nr})^{ab}/L$ of $(k_\pi k_d^{nr})^{ab}/k$ corresponds, under the isomorphism

$$\mathrm{Gal}((k_\pi k_d^{nr})^{ab}/k) \to \mathfrak{G}_d(k, \phi)$$

to the subgroup

$$G = \Big\{ (a, \xi) \in \mathfrak{G}_d(k, \phi) : a \in P \times H \Big\}$$

of $\mathfrak{G}_d(k, \phi)$. By lemma 14.1, the group $\mathrm{Gal}((k_\pi k_d^{nr})^{ab}/M_{d,n}(L))$, for $n \geq 1$, correspond, under the same isomorphism, to the group G^n.

We prove by induction on n that

$$1 \times B_{d,n+1}(H) \subseteq G^n \subseteq 1 \times B_{d,n}(H) \tag{14.2}$$

It is evident that these inclusions imply the statement of the lemma.

Let $(a, \xi), (b, \eta) \in G$. Write $a = \pi^\nu u$, $b = \pi^\mu v$ for $\nu, \mu \in \hat{\mathbb{Z}}$, $u, v \in H$. Then

$$[(a, \xi), (b, \eta)] = (1, \frac{\xi}{\phi^{-\mu}\xi \circ \{v\}} \cdot \frac{\phi^{-\nu}\eta \circ \{u\}}{\eta})$$

This expression belongs to $\mathfrak{G}_d(k, \phi)$. Therefore the power series in the second coordinate belongs to $\mathbb{F}_{q^d}[[X]]^\times = B_{d,1}(H)$. It follows that

$$G' \subseteq 1 \times B_{d,1}(H) \tag{14.3}$$

Now, take $(1, \eta) \in G$. Then $\eta \in \mathbb{F}_{q^d}[[X]]^\times$. As $\mu = 0$ and $v = 1$, we get

$$[(a, \xi), (1, \eta)] = (1, \frac{\phi^{-\nu}\eta \circ \{u\}}{\eta}) \tag{14.4}$$

Since $\pi^\nu \in P$ and $P \leq \langle \pi^d \rangle$, $\phi^{-\nu}$ acts trivially on $\mathbb{F}_{q^d}[[X]]^\times$, thus the equation (14.4) gets the form

$$[(a, \xi), (1, \eta)] = (1, \frac{\eta \circ \{u\}}{\eta}) \tag{14.5}$$

The group generated by these elements is contained in G'. But this group is exactly $1 \times B_{d,2}(H)$, and this and (14.3) imply (14.2) for $n = 1$.

Now assume (14.2) for $n \geq 1$. G^{n+1} is generated by all the commutators $[(a,\xi),(1,\eta)]$ for $(1,\eta) \in G^n$. By the induction hypothesis, $\eta \in B_{d,n}(H)$, and by (14.5), such a commutator has its second coordinate in $B_{d,n+1}(H)$.

If $\eta \in B_{d,n+1}(H)$, then by the induction hypothesis $(1,\eta) \in G^n$. Let $(\eta \circ \{u\})/\eta$ be a generator of $B_{d,n+2}(H)$. Choose $(a,\xi) \in G$ where $a = \pi^\nu u$ for $\pi^\nu \in P$ (it is already known that such a choice is always possible). Then by (14.5), the commutator $[(a,\xi),(1,\eta)]$ has its second coordinate equal to the given generator, and belongs, of course, to G^{n+1}. Hence the assertion follows. □

Proposition 14.4. *Let $H \leq U$, $P \leq \langle \pi^d \rangle^{\hat{\mathbb{Z}}}$ be closed subgroups, and let L be the field corresponding to $P \times H$ by (abelian) local class field theory, as in the previous lemma.*

Then $N_{d,\omega}(H)$ is the maximal pro-nilpotent extension over L contained in $(k_\pi k_d^{nr})^{ab}$.

Proof. By lemma 14.3, $N_{d,n}(H) \subseteq M_{d,n}(L)$ for every n, thus $N_{d,\omega}(H) \subseteq M_{d,\omega}(L)$. By the same lemma, $N_{d,n+1}(H) \supseteq M_{d,n}(L)$ for every n, hence $N_{d,\omega}(H) \supseteq M_{d,\omega}(L)$.

By lemma 14.2, $M_{d,\omega}(L)$ is the maximal pro-nilpotent extension over L contained in $(k_\pi k_d^{nr})^{ab}$, and the proposition follows. □

Remark. By the last proposition, we see that the maximal pro-nilpotent extension over L in $(k_\pi k_d^{nr})^{ab}$ does not depend on the group P.

15 Applications to the Extensions $(Kk_\pi)^{ab}/K$

We will now use the results of the previous sections to describe the maximal pro-nilpotent extension over K contained in $(Kk_\pi)^{ab}$ for a non-ramified extension K/k.

We start by computing the group $B_{d,\omega}(U_1)$ for the subgroup U_1 of the principal units in U.

Lemma 15.1. *Let $n \geq 2$. Then $B_{d,n}(U_1) \subseteq 1 + X^n \mathbb{F}_{q^d}[[X]]$.*

Proof. We prove this by induction on n. Let $\xi \in \mathbb{F}_{q^d}[[X]]^\times$, $u \in U_1$. Then $\{u\} \equiv X \pmod{X^2}$. It follows that

$$\frac{\xi \circ \{u\}}{\xi} \equiv \frac{\xi \circ X}{\xi} = 1 \pmod{X^2}$$

and the proof for $n = 2$ is complete.

Assume the statement of the lemma for n. Let $\xi \in B_{d,n}(U_1)$, $u \in U_1$. By the induction hypothesis, $\xi = 1 + X^n \xi_1$ for $\xi_1 \in \mathbb{F}_{q^d}[[X]]^\times$. Hence

$$\xi \circ \{u\} = 1 + \{u\}^n \cdot (\xi_1 \circ \{u\})$$

Since $u \in U_1$, we have $u \equiv X \pmod{X^2}$, hence $\{u\}^n \equiv X^n \pmod{X^{n+1}}$. We get that the coefficient of X^n in $\xi \circ \{u\}$ equals the constant term of ξ_1.

As $\xi = 1 + X^n \xi_1$, the coefficient of X^n in ξ also equals the constant term of ξ_1. It follows that both ξ and $\xi \circ \{u\}$ have their X^n coefficient equal. Since they are both congruent to 1 modulo X^n, we conclude that

$$\xi \circ \{u\} \equiv \xi \pmod{X^{n+1}}$$

and therefore

$$\frac{\xi \circ \{u\}}{\xi} \equiv 1 \pmod{X^{n+1}}$$

$\square$

Proposition 15.2. $B_{d,\omega}(U_1) = 1$.

Proof. By the previous lemma,

$$B_{d,\omega}(U_1) = \bigcap_{n \geq 2} B_{d,n}(U_1) \subseteq \bigcap_{n \geq 2} (1 + X^n \mathbb{F}_{q^d}[[X]]^\times) = 1$$

$\square$

Proposition 15.3. *Let K/k be a finite non-ramified extension. Then the extension $(Kk_\pi)^{ab}/(Kk_\pi^0)$ is pro-nilpotent.*

Proof. Write $K = k_d^{nr}$. As

$$\mathrm{Gal}(k^{ab}/k_d^{nr} k_\pi^0) = \langle \pi^d \rangle^{\hat{\mathbb{Z}}} \times U_1$$

we can apply proposition 14.4 and get that the maximal pro-nilpotent extension over $k_d^{nr} k_\pi^0$ in $(k_d^{nr} k_\pi)^{ab}$ equals $N_{d,\omega}(U_1)$. But by the definition of the groups $N_{d,\omega}(H)$ and proposition 15.2,

$$\mathrm{Gal}((k_d^{nr} k_\pi)^{ab}/N_{d,\omega}(U_1)) = B_{d,\omega}(U_1) = 1$$

hence $N_{d,\omega}(U_1) = (k_d^{nr} k_\pi)^{ab}$. $\square$

We can generalize proposition 15.3 and omit the assumption that K/k is finite. In order to do that, we need some lemmas.

Lemma 15.4. *Let $d_1, d_2 \geq 1$. Then $k_{d_1}^{nr} k_{d_2}^{nr} = k_{\mathrm{lcm}(d_1,d_2)}^{nr}$.*

Proof. Write $g = \gcd(d_1, d_2)$, $l = \operatorname{lcm}(d_1, d_2)$. Since $d_1 \mid l$, $d_2 \mid l$, the field k_l^{nr} contains $k_{d_1}^{nr}$ and $k_{d_2}^{nr}$ and therefore contains their compositum.

By a similar argument, k_g^{nr} is contained in $k_{d_1}^{nr}$ and $k_{d_2}^{nr}$. Now, $[k_{d_1}^{nr} : k_g^{nr}] = d_1/g$, $[k_{d_2}^{nr} : k_g^{nr}] = d_2/g$. Since d_1/g and d_2/g are relatively prime, the compositum satisfies

$$[k_{d_1}^{nr} k_{d_2}^{nr} : k_g^{nr}] = d_1 d_2 / g^2 = l/g$$

thus $[k_{d_1}^{nr} k_{d_2}^{nr} : k] = l$ and we get the required equality. □

Proposition 15.5. *Let K/k be non-ramified. Then K is a union of an increasing sequence of finite non-ramified extensions over k.*

Proof. K is a compositum of finite non-ramified extensions k_d^{nr}. Order these extensions in a sequence $\{k_{d_n}^{nr}\}$, and define,

$$\begin{aligned} e_1 &= d_1 \\ e_2 &= \operatorname{lcm}(d_1, d_2) \\ &\vdots \\ e_n &= \operatorname{lcm}(d_1, d_2, \ldots, d_n) \end{aligned}$$

By the last lemma, K equals the compositum of $\{k_{e_n}^{nr}\}$, which is an increasing sequence of fields. □

Proposition 15.6. *Let $\{L_n\}$ be an increasing sequence of fields. Let $L = \cup_{n=1}^{\infty} L_n$ and assume that the extensions L/L_n are abelian.*

Then

$$L^{ab} = \bigcup_{n=1}^{\infty} L_n^{ab}$$

Proof. We prove that for every finite abelian extension M/L, there is an n for which $M \subseteq L_n^{ab}$.

Let M/L be such an extension. Since M/L is Galois and finite, there is a polynomial $f(X) \in L[X]$ such that M is the splitting field of $f(X)$ over L. As L is the union of all L_n and the number of coefficients in $f(X)$ is finite, there is an n for which $f(X) \in L_n[X]$.

Let M' be the splitting field of $f(X)$ over L_n. Then $M = LM'$ and

$$\begin{aligned} \operatorname{Gal}(M/L \cap M') &= \operatorname{Gal}(M/L) \times \operatorname{Gal}(M/M') \\ &\cong \operatorname{Gal}(M/L) \times \operatorname{Gal}(L/L \cap M') \end{aligned}$$

Since M/L and $L/L \cap M'$ are abelian (the Galois group of the latter extension is a subgroup of $\operatorname{Gal}(L/L_n)$), we get that $\operatorname{Gal}(M/L \cap M')$ is abelian. But

$L \cap M'/L_n$ is finite, hence there is n' for which $L \cap M' \subseteq L_{n'}$. We conclude that

$$\mathrm{Gal}(M/L_{n'}) \subseteq \mathrm{Gal}(M/L \cap M')$$

is abelian. $\square$

Theorem 15.7. *Let K/k be non-ramified.*
Then the extension $(Kk_\pi)^{ab}/(Kk_\pi^0)$ is pro-nilpotent.

Proof. Proposition 15.3 states that the theorem is true in the case that K/k is finite. In the general case, write K as the union of an increasing sequence of finite non-ramified extensions K_n/k.

By proposition 15.3, for every $n \geq 1$,

$$\mathrm{Gal}((K_n k_\pi)^{ab}/(Kk_\pi^0)) \subseteq \mathrm{Gal}((K_n k_\pi)^{ab}/(K_n k_\pi^0))$$

is pro-nilpotent.

The sequence $L_n = K_n k_\pi$ satisfies the conditions of proposition 15.6 (take $L = Kk_\pi$), therefore

$$(Kk_\pi)^{ab} = \bigcup_{n=1}^{\infty} (K_n k_\pi)^{ab}$$

It follows that $\mathrm{Gal}((Kk_\pi)^{ab}/(Kk_\pi^0))$ is the inverse limit of the pro-nilpotent groups $\mathrm{Gal}((K_n k_\pi)^{ab}/(Kk_\pi^0))$, hence it is also pro-nilpotent. $\square$

Proposition 15.8. *Let V be the group of the $(q-1)$-th roots of unity in U. Then*

$$B_{d,\omega}(U) = B_{d,\omega}(V)$$

Proof. By $U = V \times U_1$ and propositions 13.5 and 15.2,

$$B_{d,\omega}(U) = B_{d,\omega}(V) B_{d,\omega}(U_1) = B_{d,\omega}(V)$$

$\square$

By local class field theory, $k_\pi/k = U$. Let L be the field for which $k_\pi/L = V$. From $U/V \cong U_1$ and the fact that U_1 is a pro-p group, we get that L/k is a pro-p extension. Moreover, since V has an order relatively prime to p, it follows that L/k is the maximal pro-p extension contained in k_π. We denote L by $k_{\pi,p}$.

Theorem 15.9. *Let K/k be non-ramified. Then the maximal pro-nilpotent extension over K contained in $(Kk_\pi)^{ab}$ equals the maximal pro-nilpotent extension over $k_{\pi,p}k^{nr}$ contained in $(Kk_\pi)^{ab}$.*

Proof. Let $k_d^{nr} \subseteq K$, and apply proposition 14.4 for the fields K and $k_{\pi,p}k^{nr}$. We get that

$$M_{d,\omega}(K) = N_{d,\omega}(U)$$

and

$$M_{d,\omega}(k_{\pi,p}k^{nr}) = N_{d,\omega}(V)$$

hence, by proposition 15.8, the maximal pro-nilpotent extension over K contained in $(k_d^{nr}k_\pi)^{ab}$ equals the maximal pro-nilpotent extension over $k_{\pi,p}k^{nr}$ contained in the same field.

Since $(Kk_\pi)^{ab}$ can be written as a union of fields $(k_d^{nr}k_\pi)^{ab}$ (cf. the proof of theorem 15.7), our theorem follows. □

Corollary. *The extensions $k_{\pi,p}^{ab}/k$ and $(k_{\pi,p}k^{nr})^{ab} \cap k_\pi^{ab}/k$ are pro-nilpotent.*

Proof. Since

$$k_{\pi,p}^{ab} \subseteq (k_{\pi,p}k^{nr})^{ab} \cap k_\pi^{ab}$$

it is enough to prove it for the latter extension. Now, $(k_{\pi,p}k^{nr})^{ab} \cap k_\pi^{ab}$ is abelian over $k_{\pi,p}k^{nr}$ (and in particular, pro-nilpotent), contained in k_π^{ab}, and the corollary follows by taking $K = k$ in theorem 15.9. □

It may be interesting to describe explicitly the subgroups $B_{d,\omega}(V)$. Here is a result in this direction.

Proposition 15.10. *Let $v \in V$ be a generator. Let λ be the homomorphism*

$$\lambda : \mathbb{F}_{q^d}[[X]]^\times \longrightarrow \mathbb{F}_{q^d}[[X]]^\times$$
$$\lambda : \xi \longmapsto \frac{\xi \circ \{v\}}{\xi}$$

Then for every $n \geq 0$,

$$B_{d,n+1}(V) = \operatorname{Im} \lambda^n$$

In particular, $B_{d,\omega}(V) = \bigcap_{n\geq 1} \operatorname{Im} \lambda^n$.

Proof. We prove this by induction on n. The proposition is trivial for $n = 0$. For the induction step, we prove that

$$B_{d,n+1}(V) = \lambda(B_{d,n}(V)) \tag{15.1}$$

Since $(\xi \circ \{v\})/\xi \in B_{d,n+1}(V)$ (this is one of the generators of $B_{d,n+1}(V)$), the inclusion $\subseteq$ follows. Now, let

$$\frac{\xi \circ \{v^i\}}{\xi}$$

be a generator of $B_{d,n+1}(V)$, and write it as

$$\frac{\xi \circ \{v^i\}}{\xi} = \prod_{j=0}^{i-1} \frac{(\xi \circ \{v^j\}) \circ \{v\}}{\xi \circ \{v^j\}}$$

It follows that this generator belongs to $\lambda(B_{d,n}(V))$, and the opposite inclusion is proved.

Finally, by $B_{d,n}(V) = \operatorname{Im} \lambda^n$ and (15.1) we get $B_{d,n+1}(V) = \operatorname{Im} \lambda^{n+1}$. $\square$

We can give also a topological description of $B_{d,\omega}(V)$.

Lemma 15.11. *The set of functions $\{\lambda^n\}$ is equicontinuous.*

Proof. For every $r \geq 1$, denote by I_r the group $1+X^r\mathbb{F}_{q^d}[[X]]$. It is sufficient to prove that for every $r \geq 1$ and $n \geq 1$,

$$\lambda^n(I_r) \subseteq I_r$$

If $\xi \in I_r$, then since $\{v\}$ is divisible by X, we have that $\xi \circ \{v\} \in I_r$, hence $\lambda(\xi) \in I_r$. Therefore $\lambda^n(\xi) \in I_r$ for every $n \geq 1$. $\square$

Proposition 15.12. *The group $B_{d,\omega}(V)$ equals the set of all limit points of the sequences $\{\lambda^n(\xi)\}$, $\xi \in \mathbb{F}_{q^d}[[X]]^\times$.*

Proof. Let η be a limit point of a sequence $\{\lambda^n\xi\}$. There is a subsequence $\lambda^{n_k}\xi \to \eta$, and since $\operatorname{Im} \lambda^n$ is a decreasing sequence of closed subgroups, η lies in their intersection, which equals $B_{d,\omega}(V)$ by proposition 15.10.

Conversely, let $\eta \in B_{d,\omega}(V)$. By proposition 15.10, for every $n \geq 1$, there is ξ_n for which $\eta = \lambda^n\xi_n$. The sequence $\{\xi_n\}$ has a convergent subsequence $\xi_{n_k} \to \xi$, and by the equicontinuity of the functions λ^n, we have $\lambda^{n_k}\xi \to \eta$. Therefore η is a limit point of a sequence $\{\lambda^n\xi\}$. $\square$

References

[Co] Coleman R., Division values in local fields, *Inv. Math.*, **53** (1979), 91–116.

[dS–K] de-Shalit E., Koch H., Metabelian local class field theory, to appear in *J. Crelle*.

[Iw] Iwasawa K., *Local Class Field Theory*, Oxford University Press, New York, 1986.

[L–T] Lubin J., Tate J., Formal complex multiplication in local fields, *Ann. Math.*, **81** (1965), 380–387.