ANNALES DE L'INSTITUT FOURIER

ANNALES

DE

L'INSTITUT FOURIER

Victor ABRASHKIN

Groups of automorphisms of local fields of period p^M and nilpotent class $< p$

Article à paraître, mis en ligne le 22 septembre 2016, 31 p.

Ann. Inst. Fourier, Grenoble
Article à paraître
Mis en ligne le 22 septembre 2016.

GROUPS OF AUTOMORPHISMS OF LOCAL FIELDS OF PERIOD p^M AND NILPOTENT CLASS $< p$

by Victor ABRASHKIN

Abstract. — Suppose K is a finite field extension of $\mathbb{Q}_p$ containing a p^M-th primitive root of unity. For $1 \leqslant s < p$ denote by $K[s, M]$ the maximal p-extension of K with the Galois group of period p^M and nilpotent class s. We apply the nilpotent Artin–Schreier theory together with the theory of the field-of-norms functor to give an explicit description of the Galois groups of $K[s, M]/K$. As application we prove that the ramification subgroup of the absolute Galois group of K with the upper index v acts trivially on $K[s, M]$ iff $v > e_K(M + s/(p - 1)) - (1 - \delta_{1s})/p$, where e_K is the ramification index of K and δ_{1s} is the Kronecker symbol.

Résumé. — Soit K une extension finie de $\mathbb{Q}_p$ contenant une racine p^M-ième primitive de l'unité. Pour $1 \leqslant s < p$ on note $K[s, M]$ la p-extension maximale de K dont le groupe de Galois est de période p^M et de classe de nilpotence s. En utilisant la théorie d'Artin–Schreier nilpotente et la théorie du corps des normes on donne une description explicite du groupe de Galois de $K[s, M]/K$. Comme application de ce résultat on montre que le sous-groupe de ramification du groupe de Galois absolu de K de ramification supérieure v agit trivialement sur $K[s, M]$ si et seulement si $v > e_K(M + s/(p - 1)) - (1 - \delta_{1s})/p$, où e_K est l'indice de ramification de K et δ_{1s} est le symbole de Kronecker.

Introduction

Everywhere in the paper $M \in \mathbb{N}$ is fixed and $p \neq 2$ is prime.

Let K be a complete discrete valuation field of characteristic 0 with finite residue field $k \simeq \mathbb{F}_{q_0}$, where $q_0 = p^{N_0}$, $N_0 \in \mathbb{N}$. Fix an algebraic closure $\bar{K}$ of K and denote by $K_{<p}(M)$ the maximal p-extension of K in $\bar{K}$ with the Galois group of nilpotent class $< p$ and exponent p^M. Then $\Gamma_{<p}(M) := \mathrm{Gal}(K_{<p}(M)/K) = \Gamma/\Gamma^{p^M} C_p(\Gamma)$, where $\Gamma = \mathrm{Gal}(\bar{K}/K)$ and $C_p(\Gamma)$ is the closure of the subgroup of commutators of order $\geqslant p$.

Keywords: local fields, upper ramification numbers.
Math. classification: 11S15, 11S20.

Let $\{\Gamma^{(v)}\}_{v\geqslant 0}$ be the ramification filtration of Γ in upper numbering [14]. The importance of this additional structure on the Galois group Γ (which reflects arithmetic properties of K) can be illustrated by the local analogue of the Grothendieck Conjecture [5, 6, 13]: the knowledge of Γ together with the filtration $\{\Gamma^{(v)}\}_{v\geqslant 0}$ is sufficient to recover uniquely the isomorphic class of K in the category of complete discrete valuation fields.

Let $\{\Gamma_{<p}(M)^{(v)}\}_{v\geqslant 0}$ be the induced ramification filtration of $\Gamma_{<p}(M)$. Then the problem of arithmetical description of $\Gamma_{<p}(M)$ is the problem of explicit description of the filtration $\{\Gamma_{<p}(M)^{(v)}\}_{v\geqslant 0}$ in terms of generators of $\Gamma_{<p}(M)$.

An analogue of this problem was studied in [2, 3, 4] in the case of local fields $\mathcal{K}$ of characteristic p with residue field k. More precisely, let $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$ and $\mathcal{G}_{<p}(M) = \mathcal{G}/\mathcal{G}^{p^M}C_p(\mathcal{G})$. In [2, 3] we developed a nilpotent version of the Artin–Schreier theory which allows us to construct identification of profinite groups $\mathcal{G}_{<p}(M) = G(\mathcal{L})$. Here $\mathcal{L}$ is a profinite Lie $\mathbb{Z}/p^M$-algebra of nilpotent class $< p$ and $G(\mathcal{L})$ is the pro-p-group, obtained from $\mathcal{L}$ by the Campbell–Hausdorff composition law, cf. Subsection 1.2 below for more details and [7, Subsection 1.1] for non-formal comments about nilpotent Artin–Schreier theory.

On the one hand, the above identification of $\mathcal{G}_{<p}(M)$ with $G(\mathcal{L})$ depends on a choice of uniformising element in $\mathcal{K}$ and, therefore, is not functorial (in particular, it can't be used directly to develop a nilpotent analog of classical local class field theory). On the other hand, the ramification subgroups $\mathcal{G}_{<p}(M)^{(v)}$ can be now described in terms of appropriate ideals $\mathcal{L}^{(v)}$ of the Lie algebra $\mathcal{L}$. The definition of these ideals essentially uses the extension of scalars $\mathcal{L}_k := \mathcal{L}\otimes W_M(k)$ of $\mathcal{L}$ (such operation does not exist in the category of p-groups) together with the appropriate explicit system of generators of $\mathcal{L}_k$, cf. Subsection 1.4. This justifies the advantage of the language of Lie algebras in the theory of p-extensions of local fields.

In this paper we apply the above characteristic p results to the study of similar properties in the mixed characteristic case, i.e. to the study of the group $\Gamma_{<p}(M)$ together with its ramification filtration. Our main tool is the Fontaine–Wintenberger theory of the field-of-norms functor [15]. Note also that we assume that K contains a primitive p^M-th root of unity and our methods generalize the approach from [1] where we considered the case $M = 1$. In some sense our theory can be treated as nilpotent version of Kummer's theory in the context of complete discrete valuation fields. As a result, we identify $\Gamma_{<p}(M)$ with the group $G(L)$, where L is a Lie $\mathbb{Z}/p^M$-algebra and for an appropriate ideal $\mathcal{J}$ of $\mathcal{L}$, we have the following exact

sequence of Lie algebras

$$0 \longrightarrow \mathcal{L}/\mathcal{J} \longrightarrow L \longrightarrow C_M \longrightarrow 0\,. \tag{0.1}$$

Here C_M is a cyclic group of order p^M with the trivial structure of Lie algebra over $\mathbb{Z}/p^M$.

As a first step in the study of L, we give an explicit description of the ideal $\mathcal{J}$. More generally, if $C_s(L)$ is the closure of the ideal of commutators of order $\geqslant s$ in L, then for $s \geqslant 2$, we have $C_s(L) \subset \mathcal{L}/\mathcal{J}$ and exact sequence (0.1) induces the exact sequences

$$0 \longrightarrow \mathcal{L}/\mathcal{L}(s) \longrightarrow L/C_s(L) \longrightarrow C_M \longrightarrow 0,$$

where all $\mathcal{L}(s)$ are ideals in $\mathcal{L}$. The main result of Section 3, Theorem 3.3, describes these ideals $\mathcal{L}(s)$ with $2 \leqslant s \leqslant p$ and gives in particular that $\mathcal{J} = \mathcal{L}(p)$.

Extension (0.1) splits in the category of $\mathbb{Z}/p^M$-modules and its structure can be given by explicit construction of a lift $\tau_{<p}$ of a generator of C_M to L and the appropriate differentiation $\mathrm{ad}\tau_{<p} \in \mathrm{End}(\mathcal{L}/\mathcal{J})$. The study of $\mathrm{ad}\tau_{<p}$ will be done in the next paper via methods used in the case $M = 1$ in [1].

In Section 4 we apply our approach to find for $1 \leqslant s < p$, the maximal upper ramification numbers $v(K[s,M]/K)$ of the maximal extensions $K[s,M]$ of K with Galois groups of period p^M and nilpotent class s. (The maximal upper ramification number for a finite extension K'/K in $\bar{K}$ is the maximal v_0 such that the ramification subgroups $\Gamma^{(v)}$ act trivially on K' if $v > v_0$.) This result can be stated in the following form, cf. Theorem 4.5 from Section 4:

If $[K:\mathbb{Q}_p] < \infty$ and $\zeta_M \in K$ then for $1 \leqslant s < p$,

$$v(K[s,M]/K) = e_K\left(M + \frac{s}{p-1}\right) - \frac{1-\delta_{s1}}{p}\,.$$

where e_K is the ramification index of $K/\mathbb{Q}_p$ and δ is the Kronecker symbol.

Remark. — The case $s = 1$ is very well-known and can be established without the assumption $\zeta_M \in K$. Is it possible to remove this restriction when $s > 1$?

Notation. — If $\mathfrak{M}$ is an R-module then its extension of scalars $\mathfrak{M} \otimes_R S$ will be very often denoted by $\mathfrak{M}_S$, cf. also another agreement in Subsection 1.1. Very often we drop off the indication to M from our notation and use just $K_{<p}, \Gamma_{<p}, \mathcal{G}_{<p}$ etc. instead of $K_{<p}(M), \Gamma_{<p}(M), \mathcal{G}_{<p}(M)$, etc.

1. Preliminaries

Let $\mathcal{K}$ be a complete discrete valuation field of characteristic p with residue field $k \simeq \mathbb{F}_{q_0}$, $q_0 = p^{N_0}$, and fixed uniformiser t_0. In other words, $\mathcal{K} = k((t_0))$.

As earlier, $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$, $\mathcal{K}_{<p} = \mathcal{K}_{<p}(M)$ is the subfield of $\mathcal{K}_{sep}$ fixed by $\mathcal{G}^{p^M} C_p(\mathcal{G})$ and $\mathcal{G}_{<p} = \mathcal{G}_{<p}(M) = \mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K})$. The ramification filtration of $\mathcal{G}_{<p}$ was studied in details in [2, 3, 4]. We overview these results in the next subsections.

1.1. Compatible system of lifts modulo p^M

The uniformizer t_0 of $\mathcal{K}$ gives a p-basis for any separable extension $\mathcal{E}$ of $\mathcal{K}$, i.e. $\{1, t_0, \dots, t_0^{p-1}\}$ is a basis of the $\mathcal{E}^p$-module $\mathcal{E}$. We can use t_0 to construct a functorial on $\mathcal{E}$ (and on M) system of lifts $O(\mathcal{E})(= O_M(\mathcal{E}))$ of $\mathcal{E}$ modulo p^M. Recall that these lifts appear in the form $W_M(\sigma^{M-1}\mathcal{E})[t]$, where W_M is the functor of Witt vectors of length M, σ is the Frobenius morphism of taking p-th power and $t = (t_0, 0, \dots, 0) \in W_M(\mathcal{K})$.

Note that $t \in O(\mathcal{K}) \subset W_M(\mathcal{K})$, $t \bmod p = t_0$ and $\sigma t = t^p$. The lift $O(\mathcal{K})$ is naturally identified with the algebra of formal Laurent series $W_M(k)((t))$ in the variable t with coefficients in $W_M(k)$. A lift σ of the absolute Frobenius endomorphism of $\mathcal{K}$ to $O(\mathcal{K})$ is uniquely determined by the condition $\sigma t = t^p$. For a separable extension $\mathcal{E}$ of $\mathcal{K}$ we then have an extension of the Frobenius σ from $\mathcal{E}$ to $O(\mathcal{E})(= W_M(\sigma^{M-1}\mathcal{E})[t])$. As a result, we obtain a compatible system of lifts of the Frobenius endomorphism of $\mathcal{K}_{sep}$ to $O(\mathcal{K}_{sep}) = \varinjlim_{\mathcal{E}} O(\mathcal{E})$. For simplicity, we shall denote this lift also by σ. Note that σ is induced by the standard Frobenius endomorphism $W_M(\sigma)$ of $W_M(\mathcal{K}_{sep}) \supset O(\mathcal{K}_{sep})$.

Suppose $\eta_0 \in \mathrm{Aut}\,\mathcal{K}$ and let $W_M(\eta_0)$ be the induced automorphism of $W_M(\mathcal{K})$. If $W_M(\eta_0)(t) \in O(\mathcal{K})$ then $\eta := W_M(\eta_0)|_{O(\mathcal{K})}$ is a lift of η_0 to $O(\mathcal{K})$, i.e. $\eta \in \mathrm{Aut}\, O(\mathcal{K})$ and $\eta \bmod p = \eta_0$. With the above notation and assumption (in particular, $\eta(t) \in O(\mathcal{K})$) we have even more.

Proposition 1.1. — *Suppose $\mathcal{E}$ is separable over $\mathcal{K}$, $\eta_{\mathcal{E}0} \in \mathrm{Aut}\,\mathcal{E}$ and $\eta_{\mathcal{E}0}|_{\mathcal{K}} = \eta_0$. Then $\eta_{\mathcal{E}} := W_M(\eta_{\mathcal{E}0})|_{O(\mathcal{E})}$ is a lift of $\eta_{\mathcal{E}0}$ to $O(\mathcal{E})$ such that $\eta_{\mathcal{E}}|_{O(\mathcal{K})} = \eta$.*

Proof. — Indeed, using that $O(\mathcal{E}) = W_M(\sigma^{M-1}\mathcal{E})[t]$, we obtain

$$\eta_{\mathcal{E}}(W_M(\sigma^{M-1}\mathcal{E})) = W_M(\eta_{\mathcal{E}0})(W_M(\sigma^{M-1}\mathcal{E})) \subset W_M(\sigma^{M-1}\mathcal{E})) \subset O(\mathcal{E})\,,$$

and $\eta_{\mathcal{E}}(t)=W_M(\eta_{\mathcal{E}0})(t)=W_M(\eta_0)(t)\in O(\mathcal{K})\subset O(\mathcal{E})$. So, $\eta_{\mathcal{E}}(O(\mathcal{E}))\subset O(\mathcal{E})$. Obviously, $\eta_{\mathcal{E}} \bmod p=\eta_{\mathcal{E}0}$. □

Remark. — The above lifts $\eta_{\mathcal{E}}$ commute with σ if and only if η commutes with σ, i.e. $\sigma(\eta(t))=\eta(t^p)$. In particular, if $\eta(t)=t\alpha^{p^{M-1}}$ with $\alpha\in O(\mathcal{K})$ then $\sigma(\eta(t))=t^p\alpha^{p^M}=\eta(t^p)$ (use that $\sigma(\alpha)\equiv\alpha^p \bmod pO(\mathcal{K})$).

A very special case of the above proposition appears as the following property:

If $\mathcal{E}/\mathcal{K}$ is Galois then the elements g of the group $\mathrm{Gal}(\mathcal{E}/\mathcal{K})$ *can be naturally lifted to (commuting with σ) automorphisms of $O(\mathcal{E})$ via setting $g(t)=t$. Therefore, $O(\mathcal{K}_{sep})$ has a natural structure of a $\mathcal{G}$-module, the action of $\mathcal{G}$ commutes with σ, $O(\mathcal{K}_{sep})^{\mathcal{G}}=O(\mathcal{K})$ and $O(\mathcal{K}_{sep})|_{\sigma=\mathrm{id}}=W_M(\mathbb{F}_p)$.*

Everywhere below we shall use the following simplified notation.

Notation. — If $\mathfrak{M}$ is a $\mathbb{Z}/p^M$-module and $\mathcal{E}$ is a separable extension of $\mathcal{K}$ we set $\mathfrak{M}_{\mathcal{E}}:=\mathfrak{M}_{O(\mathcal{E})}(=\mathfrak{M}\otimes_{\mathbb{Z}/p^M}O(\mathcal{E}))$. Similarly, we agree that $\mathfrak{M}_k:=\mathfrak{M}\otimes_{\mathbb{Z}/p^M}W_M(k)$.

1.2. Categories of p-groups and Lie $\mathbb{Z}/p^M$-algebras, [11, 12]

If L is a Lie $\mathbb{Z}/p^M$-algebra of nilpotent class $<p$, denote by $G(L)$ the p-group obtained from L via the Campbell-Hausdorff composition law $\circ$ defined for $l_1,l_2\in L$ via $\widetilde{\exp}(l_1\circ l_2)=\widetilde{\exp}l_1\cdot\widetilde{\exp}l_2$. Here

$$\widetilde{\exp}(x)=1+x+\dots+x^{p-1}/(p-1)!$$

is the truncated exponential from L to the quotient of the enveloping algebra $\mathcal{A}$ of L modulo the p-th power of its augmentation ideal J. (This construction of the Campbell-Hausdorff operation was introduced in [2, Subsection 1.2].)

The correspondence $L\mapsto G(L)$ induces equivalence of the categories of finite Lie $\mathbb{Z}/p^M$-algebras and finite p-groups of exponent p^M of the same nilpotent class $1\leqslant s_0<p$. This equivalence can be extended to the similar categories of profinite Lie algebras and groups.

1.3. Witt pairing and Hilbert symbol, [8, 9]

Let

$$E(\alpha,X)=\exp\left(\alpha X+\frac{\sigma(\alpha)X^p}{p}+\dots+\frac{\sigma^n(\alpha)X^{p^n}}{p^n}\dots\right)\in W(k)[\![X]\!],$$

where $\alpha \in W(k)$, be the Shafarevich version of the Artin–Hasse exponential. Set $\mathbb{Z}^+(p) = \{a \in \mathbb{N} \mid \gcd(a,p) = 1\}$. Then any element $u \in \mathcal{K}^* \mathrm{mod}\, \mathcal{K}^{*p^M}$ can be uniquely written as

$$u = t_0^{a_0} \prod_{a \in \mathbb{Z}^+(p)} E(\alpha_a, t_0^a)^{1/a} \mathrm{mod}\, \mathcal{K}^{*p^M},$$

where $a_0 = a_0(u) \in \mathbb{Z} \,\mathrm{mod}\, p^M$ and all $\alpha_a = \alpha_a(u) \in W(k) \,\mathrm{mod}\, p^M$.

Let $\mathfrak{M}$ be a profinite free $W_M(k)$-module with the set of generators $\{D_0\} \cup \{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\}$. Use the correspondences

$$t_0 \mapsto D_0, \quad E(\alpha, t_0^a)^{1/a} \mapsto \sum_{n \,\mathrm{mod} N_0} \sigma^n(\alpha) D_{an}, \tag{1.1}$$

to identify $\mathcal{K}^*/\mathcal{K}^{*p^M}$ with a closed $\mathbb{Z}/p^M$-submodule in $\mathfrak{M}$. Under this identification we have $\mathcal{K}^*/\mathcal{K}^{*p^M} \otimes_{\mathbb{Z}/p^M} W_M(k) = \mathfrak{M}$.

Define the continuous action of the group $\langle \sigma \rangle = \mathrm{Gal}(k/\mathbb{F}_p)$ on $\mathfrak{M}$ as an extension of the natural action on $W_M(k)$ by setting $\sigma D_0 = D_0$ and $\sigma D_{an} = D_{a,n+1}$. Then $\mathcal{K}^*/\mathcal{K}^{*p^M} = \mathfrak{M}^{\mathrm{Gal}(k/\mathbb{F}_p)}$.

The Witt pairing

$$O(\mathcal{K})/(\sigma - \mathrm{id})O(\mathcal{K}) \times \mathcal{K}^*/\mathcal{K}^{*p^M} \longrightarrow \mathbb{Z}/p^M,$$

is given explicitly by the symbol $[f, g) = \mathrm{Tr}\,(\mathrm{Res}(f\, d_{\log} \mathrm{Col}\, g))$. Here $\mathrm{Tr} : W_M(k) \longrightarrow \mathbb{Z}/p^M$ is induced by the trace of the field extension $k/\mathbb{F}_p$, $f \in O(\mathcal{K})$ and $\mathrm{Col}\, g$ is the image of $g \in \mathcal{K}^*/\mathcal{K}^{*p^M}$ under the group homomorphism $\mathrm{Col} : \mathcal{K}^*/\mathcal{K}^{*p^M} \longrightarrow O_M^*(\mathcal{K})$ uniquely defined on the above free generators of $\mathcal{K}^*/\mathcal{K}^{*p^M}$ via the conditions $t_0 \mapsto t$ and $E(\alpha, t_0^a) \mapsto E(\alpha, t^a)$. The Witt pairing is non-degenerate and determines the identification

$$\mathcal{K}^*/\mathcal{K}^{*p^M} = \mathrm{Hom}_{\mathrm{cont}}(O(\mathcal{K})/(\sigma - \mathrm{id})O(\mathcal{K}), \mathbb{Z}/p^M).$$

It also coincides with the Hilbert symbol (in the case of local fields of characteristic p) and allows us to specify explicitly the reciprocity map $\kappa : \mathcal{K}^*/\mathcal{K}^{*p^M} \longrightarrow \mathcal{G}_{<p}^{ab}$ of class field theory. Namely, in the above notation we have $\kappa(g)f = f + [f, g)$.

1.4. Lie algebra $\mathcal{L}$ and identification η_M

Let $\widetilde{\mathcal{L}}$ be a free profinite Lie $\mathbb{Z}/p^M$-algebra with the module of (free) generators $\mathcal{K}^*/\mathcal{K}^{*p^M}$. Then the $W_M(k)$-module $\widetilde{\mathcal{L}}_k$ has the set of free generators

$$\{D_0\} \cup \{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\}. \tag{1.2}$$

If $C_p(\widetilde{\mathcal{L}})$ is the closure of the ideal of commutators of order $\geqslant p$, then $\mathcal{L}=\widetilde{\mathcal{L}}/C_p(\widetilde{\mathcal{L}})$ is the maximal quotient of $\widetilde{\mathcal{L}}$ of nilpotent class $<p$.

Remark. — $\mathcal{L}_k$ is a free object in the category of profinite Lie $W_M(k)$-algebras of nilpotent class $<p$ with the set of free generators (1.2).

We shall use the same notation D_0 and D_{an} for the images of the elements of (1.2) in $\mathcal{L}$. Choose $\alpha_0\in W_M(k)$ such that $\operatorname{Tr}\alpha_0=1$.

Consider $e=\alpha_0 D_0+\sum_{a\in\mathbb{Z}^+(p)}t^{-a}D_{a0}\in G(\mathcal{L}_{\mathcal{K}})$. If we set $D_{0n}:=(\sigma^n\alpha_0)D_0$ then e can be written as $\sum_{a\in\mathbb{Z}^0(p)}t^{-a}D_{a0}$, where $\mathbb{Z}^0(p)=\mathbb{Z}^+(p)\cup\{0\}$.

Fix $f\in G(\mathcal{L}_{\mathcal{K}_{sep}})$ such that $\sigma f=e\circ f$. Then for $\tau\in\mathcal{G}$, the correspondence

$$\tau\mapsto(-f)\circ\tau f\in G(\mathcal{L}_{K_{sep}})|_{\sigma=\mathrm{id}}=G(\mathcal{L}),$$

induces the identification of profinite groups $\eta_M:\mathcal{G}_{<p}\simeq G(\mathcal{L})$.

Note that $f\in\mathcal{L}_{\mathcal{K}_{<p}}$ and $\mathcal{G}_{<p}$ strictly acts on the $\mathcal{G}$-orbit of f.

The above result is a covariant version of the nilpotent Artin–Schreier theory developed in [3], cf. also Subsection 1.1 in [7] for the relation between the covariant and contravariant versions of this theory and for appropriate non-formal comments.

We shall use below a fixed choice of f and use the notation for e and f without further references.

1.5. Relation to class field theory

The above identification η_M taken modulo $C_2(\mathcal{G}_{<p})$ gives an isomorphism of profinite p-groups

$$\eta_M^{ab}:\mathcal{G}_{<p}^{\mathrm{ab}}\longrightarrow\mathcal{L}^{ab}=\mathcal{L}/C_2(\mathcal{L})=\mathfrak{M}^{\mathrm{Gal}(k/\mathbb{F}_p)}=\mathcal{K}^*/\mathcal{K}^{*p^M}.$$

Proposition 1.2. — *η_M^{ab} is induced by the inverse to the reciprocity map of local class field theory κ.*

Proof. — Indeed, let $\{\beta_i\}_{1\leqslant i\leqslant N_0}$ be a $\mathbb{Z}/p^M$-basis of $W_M(k)$ and let $\{\gamma_i\}_{1\leqslant i\leqslant N_0}$ be its dual basis with respect to the bilinear form induced by the trace of the field extension $W(k)[1/p]/\mathbb{Q}_p$.

If $a\in\mathbb{Z}^+(p)$ and $E(\beta_i,t_0^a)^{1/a}=D_{ia}$, then $D_{ia}=\sum_n\sigma^n(\beta_i)D_{an}$, and, therefore, $D_{a0}=\sum_i\gamma_iD_{ia}$. This implies that

$$e=\sum_{i,a}t^{-a}\gamma_iD_{ia}+\alpha_0D_0 \bmod C_2(\mathcal{L}_{\mathcal{K}}),$$

$$f=\sum_{i,a}f_{ia}D_{ia}+f_0D_0 \bmod C_2(\mathcal{L}_{\mathcal{K}_{sep}}),$$

where all $f_{ia}, f_0 \in O(\mathcal{K}_{<p})$, $\sigma f_{ia} - f_{ia} = \gamma_i t^{-a}$ and $\sigma f_0 - f_0 = \alpha_0$. From the definition of η_M it follows formally that for $\tau_{ia} = (\eta_M^{ab})^{-1} D_{ia}$ and $\tau_0 = (\eta_M^{ab})^{-1} D_0$, $\tau_{ia} f_{i_1 a_1} = f_{i_1 a_1} + \delta(ii_1)\delta(aa_1)$, $\tau_0 f_{i_1 a_1} = f_{i_1 a_1}$, $\tau_{ia} f_0 = f_0$ and $\tau_0 f_0 = f_0 + 1$. (Here δ is the Kronecker symbol.)

Now the explicit formula for the Hilbert symbol from Subsection 1.3 shows that $\kappa(E(\beta_i, t_0^a)^{1/a})$ and $\kappa(t_0)$ act by the same formulae as τ_{ia} and, resp., τ_0. □

1.6. Construction of lifts of analytic automorphisms

Let $\eta_0 \in \mathrm{Aut}\mathcal{K}$. Then there is a lift $\eta_{<p,0} \in \mathrm{Aut}\mathcal{K}_{<p}$ of η_0. (Use that the subgroup $\mathcal{G}^{p^M} C_p(\mathcal{G})$ of $\mathcal{G}$ is characteristic.) For any another such lift $\eta'_{<p,0}$, we have $\eta'_{<p,0}\eta_{<p,0}^{-1} \in \mathcal{G}_{<p}$.

The covariant version of the Witt–Artin–Schreier theory [3], Section 1 (cf. also [7, Subsection 1.1] and [1, Section 1]), gives explicit description of the automorphisms $\eta_{<p,0}$ in terms of the identification η_M. Consider a special case of this construction when η_0 admits a lift $\eta \in \mathrm{Aut}\, O(\mathcal{K})$ which commutes with σ, and therefore we have the appropriate lifts $\eta_{<p} \in \mathrm{Aut}\, O(\mathcal{K}_{<p})$, cf. Subsection 1.1. Then in terms of our fixed elements e and f, we have $\eta_{<p}(f) = c \circ (A \otimes \mathrm{id}_{O(\mathcal{K}_{<p})}) f$, where $c \in \mathcal{L}_{\mathcal{K}}$ and $A \in \mathrm{Aut}\mathcal{L}$ can be found from the relation

$$(\mathrm{id}_{\mathcal{L}} \otimes \eta)e = \sigma c \circ (A \otimes \mathrm{id}_{O(\mathcal{K})})e \circ (-c)\,,$$

cf. [3, Subsection 1.5], or [1, Proposition 1.1], and Subsection 3.2 below.

In other words, if $(A \otimes \mathrm{id}_{W_M(k)})(D_{a0}) = \widetilde{D}_{a0}$ then

$$\sum_{a \in \mathbb{Z}^0(p)} \eta(t)^{-a} D_{a0} = \sigma c \circ \left(\sum_{a \in \mathbb{Z}^0(p)} t^{-a} \widetilde{D}_{a0} \right) \circ (-c)\,.$$

Note that proceeding as in [3, Subsection 1.5.4], cf. also [1, Subsection 1.2], we can verify (this fact will be used systematically below) that with respect to the identification η_M, the automorphism A coincides with the conjugation $\mathrm{Ad}\,\eta_{<p} : \tau \mapsto \eta_{<p}^{-1}\, \tau\, \eta_{<p}$ (here $\tau \in \mathcal{G}_{<p}$).

1.7. Ramification filtration in $\mathcal{L}$

For $v \geqslant 0$, denote by $\mathcal{G}_{<p}^{(v)}$ the ramification subgroup of $\mathcal{G}_{<p}$ with the upper index v. Let $\mathcal{L}^{(v)}$ be the ideal of $\mathcal{L}$ such that $\eta_M(\mathcal{G}_{<p}^{(v)}) = G(\mathcal{L}^{(v)})$. The ideals $\mathcal{L}^{(v)}$ have the following explicit description.

First, for any $a \in \mathbb{Z}^0(p)$ and $n \in \mathbb{Z}$, set $D_{an} := D_{a,n \bmod N_0}$. In other words, we allow the second index in all D_{an} to take integral values and assume that $D_{an_1} = D_{an_2}$ iff $n_1 \equiv n_2 \bmod N_0$. For $s \geqslant 1$, agree to use the notation $(\bar{a}, \bar{n})_s$, where $\bar{a} = (a_1, \dots, a_s)$ has coordinates in $\mathbb{Z}^0(p)$ and $\bar{n} = (n_1, \dots, n_s) \in \mathbb{Z}^s$. Then we can attach to $(\bar{a}, \bar{n})_s$ the commutator $[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_sn_s}]$ and set $\gamma(\bar{a}, \bar{n})_s = a_1p^{n_1} + \dots + a_sp^{n_s}$. For any $\gamma \geqslant 0$, let $\mathcal{F}^0_{\gamma,-N}$ be the element from $\mathcal{L}_k$ given by

$$\mathcal{F}^0_{\gamma,-N} = \sum_{\gamma(\bar{a},\bar{n})_s=\gamma} p^{n_1} a_1 \eta(\bar{n})[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_sn_s}] \tag{1.3}$$

where $\eta(\bar{n})$ equals $(s_1!(s_2-s_1)! \dots (s-s_l)!)^{-1}$ if $0 \leqslant n_1 = \dots = n_{s_1} > n_{s_1+1} = \dots = n_{s_2} > \dots > n_{s_l} = \dots = n_s \geqslant -N$, and equals to zero otherwise. Then the main result of [4] (translated into the covariant setting, cf. [5, Subsections 1.1.2 and 1.2.4]) states that:

> *There is $\widetilde{N}(v) \in \mathbb{N}$ such that if we fix any $N \geqslant \widetilde{N}(v)$, then $\mathcal{L}^{(v)}$ is the minimal ideal of $\mathcal{L}$ such that for all $\gamma \geqslant v$, $\mathcal{F}^0_{\gamma,-N} \in \mathcal{L}_k^{(v)}$.*

2. Filtration $\{\mathcal{L}(s)\}_{s\geqslant 1}$

In this section we define a decreasing central filtration $\{\mathcal{L}(s)\}_{s\geqslant 1}$ in the $\mathbb{Z}/p^M$-Lie algebra $\mathcal{L}$ from Subsection 1.4. Its definition depends on a choice of a special element $S \in \mathrm{m}(\mathcal{K}) := tW_M(k)[\![t]\!] \subset O(\mathcal{K})$. This element S (together with the appropriate elements S_0 and S' from its definition) will be specified in Section 4, where we apply our results to the mixed characteristic case.

2.1. Elements $S_0, S', S \in \mathrm{m}(\mathcal{K})$

Let $[p]$ be the isogeny of multiplication by p in the formal group $\operatorname{Spf} \mathbb{Z}_p[\![X]\!]$ over $\mathbb{Z}_p$ with the logarithm $X + X^p/p + \dots + X^{p^n}/p^n + \dots$.

Choose $S_0 \in \mathrm{m}(\mathcal{K})$ and set $S' = [p]^{M-1}(S_0)$ and $S = [p]^M(S_0)$. Then $S, S' \in \mathrm{m}(\mathcal{K})$, they both depend only on the residue $S_0 \bmod p$ and $S = \sigma S'$. In particular, if $e^* \in \mathbb{N}$ is such that $S \bmod p$ generates the ideal $(t_0^{e^*})$ in $k[\![t_0]\!]$ then $e^* \equiv 0 \bmod p^M$.

PROPOSITION 2.1.

(a) $dS = 0$ *in* $\Omega^1_{O(\mathcal{K})}$;

(b) *there is* $S'' \in \mathrm{m}(\mathcal{K})$*, such that* $S = S'(p + S'')$*;*

(c) *there are* $\eta_0, \eta_1 \in W_M(k)[\![t]\!]^\times$ *and* $\eta_2 \in W_M(k)[\![t]\!]$ *such that*

$$S = t^{e^*}\eta_0 + pt^{e^*/p}\eta_1 + p^2\eta_2.$$

Proof.

(a) The congruence $[p]X \equiv X^p \bmod p\mathbb{Z}_p[\![X]\!]$ implies that $d([p]X) \in p\mathbb{Z}_p[\![X]\!]$. Therefore, $dS = 0$ in $\Omega^1_{O(\mathcal{K})}$.

(b) Note that $[p](X) \equiv pX \bmod X^2$. Therefore, there are $w_i \in \mathbb{Z}_p$ such that $S = [p]S' = pS' + \sum_{i\geqslant 2} w_i S'^i$ and we can take $S'' = \sum_{i\geqslant 1} w_{i+1}S'^i$.

(c) The t_0-adic valuation of $S' \bmod p$ equals e^*/p. Then our property is implied by the following equivalence in $\mathbb{Z}_p[\![X]\!]$

$$[p](X) \equiv pX + X^p \bmod (pX^{p^2-p+1}, p^2X). \qquad \square$$

Remark. — We shall use below property (a) in the following form:

If $s \in \mathbb{N}$ *and* $S^s = \sum_{l\geqslant 1} \gamma_{ls}t^l$*, where all* $\gamma_{ls} \in W_M(k)$*, then* $l\gamma_{ls} = 0$.

2.2. Morphism ι

Let $\mathcal{U} = (1 + t_0k[\![t_0]\!])^\times$ be the $\mathbb{Z}_p$-module of principal units in $\mathcal{K}$. Then $\mathcal{U}/\mathcal{U}^{p^M}$ is a closed $\mathbb{Z}/p^M$-submodule in $\mathcal{K}^*/\mathcal{K}^{*p^M}$. Note that $\mathrm{m}(\mathcal{K}) = W_M(\mathrm{m}_\mathcal{K}) \cap O(\mathcal{K})$, where $\mathrm{m}_\mathcal{K}$ is the maximal ideal in the valuation ring of $\mathcal{K}$. Consider a (unique) continuous homomorphism

$$\iota : \mathcal{U} \longrightarrow \mathrm{m}(\mathcal{K})$$

such that for any $\alpha \in W_M(k)$ and $a \in \mathbb{Z}^+(p)$, $\iota : E(\alpha, t_0^a) \mapsto \alpha t^a$ (here E is the Shafarevich function, cf. Subsection 1.3).

Then ι induces an identification of $\mathcal{U}/\mathcal{U}^{p^M}$ with the closed $W_M(k)$-submodule

$$\mathrm{Im}\,\iota = \left\{ \sum_{a\in\mathbb{Z}^+(p)} \alpha_a t^a \,\middle|\, \alpha_a \in W_M(k) \right\}$$

in $O(\mathcal{K})$. This submodule is topologically generated over $W_M(k)$ by all t^a with $a \in \mathbb{Z}^+(p)$.

2.3. Definition of $\{\mathcal{L}(s)\}_{s\geqslant 1}$

Set $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(1)}=\mathcal{K}^*/\mathcal{K}^{*p^M}$. For $s\geqslant 1$, let $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}=(\mathrm{Im}\,\iota)S^s$ with respect to the identification $\mathcal{U}/\mathcal{U}^{p^M}=\mathrm{Im}\,\iota$ from Subsection 2.2. Note, that $S=\sigma S'$ implies that for any $s\in\mathbb{N}$, $(\mathrm{Im}\,\iota)S^s\subset\mathrm{Im}\,\iota$.

Definition. — *$\{\mathcal{L}(s)\}_{s\geqslant 1}$ is the minimal central filtration of ideals of the Lie algebra $\mathcal{L}$ such that for all $s\geqslant 1$, $\mathcal{L}(s)\supset(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}$.*

The ideals $\mathcal{L}(s)$ can be defined by induction on s as follows. Let $\mathcal{L}(1)=\mathcal{L}$; then for $s\geqslant 1$, the ideal $\mathcal{L}(s+1)$ is generated by the elements of $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}$ and $[\mathcal{L}(s),\mathcal{L}]$. Note also that for any s, $(\mathcal{K}^*/\mathcal{K}^{*p^M})\cap\mathcal{L}(s)=(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}$. (Use that $\mathbb{Z}/p^M$-module $\mathcal{L}(s)$ is isomorphic to $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}\oplus(\mathcal{L}(s)\cap C_2(\mathcal{L}))$.

In addition, for any $s\geqslant 1$, the quotients $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}/(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}$ are free $\mathbb{Z}/p^M$-modules. This easily implies that all $\mathcal{L}(s)/\mathcal{L}(s+1)$ are also free $\mathbb{Z}/p^M$-modules.

2.4. Characterization of $\{\mathcal{L}(s)\}_{s\geqslant 1}$ in terms of $e\in\mathcal{L}_{\mathcal{K}}$

Recall that $e=\sum_{a\in\mathbb{Z}^0(p)}t^{-a}D_{a0}$, cf. Subsection 1.4.

Proposition 2.2. — *The filtration $\{\mathcal{L}(s)\}_{s\geqslant 1}$ is the minimal central filtration in $\mathcal{L}$ such that $\mathcal{L}(1)=\mathcal{L}$ and for all $s\geqslant 1$,*

$$S^se\in\mathcal{L}_{\mathrm{m}(\mathcal{K})}+\mathcal{L}(s+1)_{\mathcal{K}}.$$

Proof. — We need the following two lemmas.

Lemma 2.3. — *For all $s\geqslant 1$ and $\alpha_a\in W_M(k)$ where $a\in\mathbb{Z}^+(p)$, we have*

$$\prod_{a\in\mathbb{Z}^+(p)}E(\alpha_a,t_0^a)\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}$$
$$\Leftrightarrow\prod_{a\in\mathbb{Z}^+(p)}E(\alpha_a,t_0^a)^{1/a}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}.$$

Proof of Lemma 2.3. — We must prove that

$$\sum_{a\in\mathbb{Z}^+(p)}\alpha_at^a\in S^s\mathrm{m}(\mathcal{K})\quad\Leftrightarrow\quad\sum_{a\in\mathbb{Z}^+(p)}\frac{1}{a}\alpha_at^a\in S^s\mathrm{m}(\mathcal{K}).$$

Let $S^s=\sum_{l\geqslant 1}\gamma_{ls}t^l$ with $\gamma_{ls}\in W_M(k)$, then $l\gamma_{ls}=0$, cf. Remark in Subsection 2.1.

Suppose
$$\sum_{a\in\mathbb{Z}^+(p)}\alpha_a t^a\in S^s\mathrm{m}(\mathcal{K}).$$
Then $\sum_a\alpha_a t^a=(\sum_b\beta_b t^b)(\sum_l\gamma_{ls}t^l)$, where $\sum_b\beta_b t^b\in\mathrm{m}(\mathcal{K})$ and $\alpha_a=\sum_{a=b+l}\beta_b\gamma_{ls}$. This implies
$$\frac{1}{a}\alpha_a=\sum_{a=b+l}\frac{1}{a}\beta_b\gamma_{ls}=\sum_{a=b+l}\frac{1}{b}\beta_b\gamma_{ls},$$
because if $a=b+l$ and $a\in\mathbb{Z}^+(p)$ then $b\in\mathbb{Z}^+(p)$ and
$$\frac{1}{a}\gamma_{ls}-\frac{1}{b}\gamma_{ls}=\frac{-l\gamma_{ls}}{ab}=0.$$

So,
$$\sum_{a\in\mathbb{Z}^+(p)}\frac{1}{a}\alpha_a t^a=\left(\sum_{b\in\mathbb{Z}^+(p)}\frac{1}{b}\beta_b t^b\right)\left(\sum_l\gamma_{ls}t^l\right)$$
and
$$\sum_a\frac{1}{a}\alpha_a t^a\in S^s\mathrm{m}(\mathcal{K}).$$

Proceeding in the opposite direction we obtain the inverse statement. The lemma is proved. □

Lemma 2.4. — *If $s\geqslant 1$ and all $\alpha_a\in W_M(k)$ then*
$$\prod_{a\in\mathbb{Z}^+(p)}E(\alpha_a,t_0^a)^{1/a}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}\Leftrightarrow\sum_{a\in\mathbb{Z}^+(p)}\alpha_a D_{a0}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})_k^{(s)}$$

Proof of Lemma 2.4. — Suppose
$$\prod_{a\in\mathbb{Z}^+(p)}E(\alpha_a,t_0^a)^{1/a}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}.$$

Choose a $W_M(\mathbb{F}_p)$-basis $\{\beta_i\}$ of $W_M(k)$, and let $\{\gamma_i\}$ be its dual with respect to the trace form. Then for any i,
$$\prod_{a\in\mathbb{Z}^+(p)}E(\beta_i\alpha_a,t_0^a)^{1/a}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}.$$

In other words (use (1.1) from Subsection 1.3),
$$c_i=\sum_{\substack{a\in\mathbb{Z}^+(p)\\ n\in\mathbb{Z}/N_0\mathbb{Z}}}\sigma^n(\beta_i)\sigma^n(\alpha_a)D_{an}\in\left(\mathcal{K}^*/\mathcal{K}^{*p^M}\right)^{(s)}\subset\mathcal{L}(s),$$
and
$$\sum_i\gamma_i c_i=\sum_{a\in\mathbb{Z}^+(p)}\alpha_a D_{a0}\in\mathcal{L}(s)_k.$$

Suppose now that $\sum_{a\in\mathbb{Z}^+(p)}\alpha_a D_{a0}\in\mathcal{L}(s)_k$. Then

$$\sum_{a\in\mathbb{Z}^+(p)}\alpha_a D_{a0}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})_k^{(s)},$$

and, therefore,

$$\sum_{\substack{a\in\mathbb{Z}^+(p)\\ n\in\mathbb{Z}/N_0\mathbb{Z}}}\sigma^n(\alpha_a)D_{an}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}.$$

This means, that

$$\prod_{a\in\mathbb{Z}^+(p)}E(\alpha_a,t_0^a)^{1/a}\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}.$$

The lemma is proved. □

Now we can finish the proof of our proposition. If, as earlier, $S^s=\sum_{l\geqslant 1}\gamma_{ls}t^l$ with $\gamma_{ls}\in W_M(k)$, then $(\operatorname{Im}\iota)S^s$ is the $W_M(k)$-submodule in $\mathrm{m}(\mathcal{K})$ generated by the elements $t^{a_1}S^s=\sum_{l\geqslant 1}\gamma_{ls}t^{l+a_1}$, $a_1\in\mathbb{Z}^+(p)$. The above lemmas imply then that $\{\mathcal{L}(s)\}_{s\geqslant 1}$ is the minimal central filtration in $\mathcal{L}$ such that $\mathcal{L}(1)=\mathcal{L}$ and for all $a_1\in\mathbb{Z}^+(p), s\geqslant 1$,

$$\sum_{l\geqslant 1}\gamma_{ls}D_{a_1+l,0}\in\mathcal{L}(s+1)_k\,.$$

On the other hand,

$$S^se=\sum_{\substack{a\in\mathbb{Z}^0(p)\\ l\geqslant 1}}\gamma_{ls}t^{-(a-l)}D_{a0}\equiv\sum_{a_1\in\mathbb{Z}^+(p)}\left(\sum_{l\geqslant 1}\gamma_{ls}D_{a_1+l,0}\right)t^{-a_1}$$

modulo $\mathcal{L}_{\mathrm{m}(\mathcal{K})}$. Therefore,

$$S^se\in\mathcal{L}_{\mathrm{m}(\mathcal{K})}+\mathcal{L}(s+1)_{\mathcal{K}}$$
$$\Leftrightarrow\sum_l\gamma_{ls}D_{a_1+l,0}\in\mathcal{L}(s+1)_k\quad\text{for all } a_1\in\mathbb{Z}^+(p).$$

The proposition is proved. □

Definition. — $\mathcal{N}=\sum_{s\geqslant 1}S^{-s}\mathcal{L}(s)_{\mathrm{m}(\mathcal{K})}$.

Note that $\mathcal{N}$ is a Lie $W_M(\mathbb{F}_p)$-subalgebra in $\mathcal{L}_{\mathcal{K}}$. With this notation Proposition 2.2 implies the following characterization of the filtration $\{\mathcal{L}(s)\}_{s\geqslant 1}$.

Corollary 2.5. — *$\{\mathcal{L}(s)\}_{s\geqslant 1}$ is the minimal central filtration in $\mathcal{L}$ such that $\mathcal{L}(1)=\mathcal{L}$ and $e\in\mathcal{N}$.*

Proof. — It will be sufficient to verify that

$$e \in \mathcal{N} \;\Leftrightarrow\; \forall s \geqslant 1,\; S^s e \in \mathcal{L}_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(s+1)_{\mathcal{K}}\,.$$

The "if" part is obvious. The "only if" part can be proved by induction on s via the following property:

If $l'(s) \in \mathcal{L}(s)_{\mathcal{K}}$ and $Sl'(s) \in \mathcal{L}_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(s+1)_{\mathcal{K}}$ then $l'(s) \in S^{-1}\mathcal{L}(s)_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(s+1)_{\mathcal{K}}$ (use that $\mathcal{L}(s)/\mathcal{L}(s+1)$ is free $\mathbb{Z}/p^M$-module). □

2.5. Element $e^{\dagger} \in G(\mathcal{L}_{\mathcal{K}})$

Recall that $S \bmod p$ generates the ideal $(t_0^{e^*})$ in $k[\![t_0]\!]$. Therefore, the projections of the elements of the set

$$\left\{S^{-m}t^b \mid 1 \leqslant b < e^*, \gcd(b,p) = 1, m \in \mathbb{N}\right\} \cup \{\alpha_0\}$$

form a basis of $O(\mathcal{K})/(\sigma - \mathrm{id})O(\mathcal{K})$ over $W_M(k)$.

Proposition 2.6. — *There are $V_{(0)} \in \mathcal{L}$, $x \in S\mathcal{N}$ and $V_{(b,m)} \in \mathcal{L}_k$, where $m \geqslant 1$, $1 \leqslant b < e^*$, $\gcd(b,p) = 1$, such that*

(a) $e^{\dagger} := \sum_{m,b} S^{-m}t^b V_{(b,m)} + \alpha_0 V_{(0)} \in \mathcal{N}$;

(b) $e^{\dagger} = (-\sigma x) \circ e \circ x$.

Proof. — Note that $S \in \sigma\mathrm{m}(\mathcal{K})$ implies that the sets $\{t^{-a} \mid a \in \mathbb{Z}^+(p)\}$ and $\{S^{-m}t^b \mid m \in \mathbb{N}, \gcd(b,p) = 1, 1 \leqslant b < e^*\}$ generate the same $W_M(k)$-submodules in $O(\mathcal{K})/\mathrm{m}(\mathcal{K})$. This implies the existence of $V_{(0)}^{(0)} \in \mathcal{L}$ and $V_{(b,m)}^{(0)} \in \mathcal{L}_k$ such that

$$e \equiv e_0^{\dagger} \bmod \mathcal{L}_{\mathrm{m}(\mathcal{K})} \tag{2.1}$$

where $e_0^{\dagger} := \sum_{(b,m)} S^{-m}t^b V_{(b,m)}^{(0)} + \alpha_0 V_{(0)}^{(0)}$.

For $i \geqslant 1$, let $\mathcal{N}^{(i)} = \sum_{s \geqslant i} S^{-s}\mathcal{L}(s)_{\mathrm{m}(\mathcal{K})}$. Then

- $\mathcal{N}^{(i)} = S^{-i}\mathcal{L}(i)_{\mathrm{m}(\mathcal{K})} + \mathcal{N}^{(i+1)}$;
- $\left[\mathcal{N}^{(i)}, \mathcal{N}\right] \subset \mathcal{N}^{(i+1)}$.

In particular, relation (2.1) implies that $e = e_0^{\dagger} + \sigma x_0 - x_0$, where $x_0 \in \mathcal{L}_{\mathrm{m}(\mathcal{K})}$, and we obtain

$$(-\sigma x_0) \circ e \circ x_0 \equiv e_0^{\dagger} \bmod S\mathcal{N}^{(2)} \tag{2.2}$$

(use that $x_0, \sigma x_0 \in \mathcal{L}_{\mathrm{m}(\mathcal{K})} \subset S\mathcal{N}^{(1)}$). Now we need the following lemma.

Lemma 2.7. — *Suppose $\mathfrak{M}$ is a $\mathbb{Z}_p$-module and $i_0 \in \mathbb{N}$. Then for any $l \in S^{-i_0}\mathfrak{M}_{\mathrm{m}(\mathcal{K})}$, there are $l_{(0)} \in \mathfrak{M}$, $\tilde{l} \in S^{-i_0}\mathfrak{M}_{\mathrm{m}(\mathcal{K})}$ and $l_{(b,m)} \in \mathfrak{M}_k$, where $1 \leqslant m \leqslant i_0$, $\gcd(p,b)=1$ and $1 \leqslant b < e^*$, such that*

$$l = \sum_{b,m} S^{-m}t^b l_{(b,m)} + \alpha_0 l_{(0)} + \sigma\tilde{l} - \tilde{l}.$$

Proof of Lemma 2.7. — It will be sufficient to consider the case $\mathfrak{M} = \mathbb{Z}_p$. In other words, we must prove the following statement:

For any $s \in S^{-i_0}\mathrm{m}(\mathcal{K})$, there are $\beta_{(0)} \in W_M(\mathbb{F}_p)$, $\tilde{s} \in S^{-i_0}\mathrm{m}(\mathcal{K})$ and $\beta_{(b,m)} \in W_M(k)$, where $1 \leqslant m \leqslant i_0$, $\gcd(b,p)=1$ and $1 \leqslant b < e^*$, such that

$$s = \sum_{b,m} \beta_{(b,m)} S^{-m}t^b + \alpha_0\beta_{(0)} + \sigma\tilde{s} - \tilde{s}.$$

We can assume that $s = t^{a_0}/S^{i_0}$, where $1 \leqslant a_0 < e^*$, $i_0 \in \mathbb{N}$ and our lemma is proved for all elements s from $pS^{-i_0}\mathrm{m}(\mathcal{K}) + t^{a_0}S^{-i_0}\mathrm{m}(\mathcal{K})$.

If $\gcd(a_0,p)=1$ there is nothing to prove. Otherwise, $a_0 = pa_1$ and $s = s' + \sigma(s') - s'$ with $s' = t^{a_1}/S'^{i_0} = t^{a_1}(p+S'')/S^{i_0}$. It remains to note that $s' \in pS^{-i_0}\mathrm{m}(\mathcal{K}) + t^{a_0}S^{-i_0}\mathrm{m}(\mathcal{K})$, because $S'' \bmod p \in (t_0^{e^0})$, where $e^0 := e^*(1-1/p)$, and $a_1 + e^0 = a_0/p + e^0 > a_0$ (use that $a_0 < e^*$). ☐

Continue the proof of Proposition 2.6. Clearly, it is implied by the following lemma.

Lemma 2.8. — *For all $i \geqslant 0$, there are $x_i \in S\mathcal{N}$, $V^{(i)}_{(b,m)} \in \mathcal{L}_k$ and $V^{(i)}_{(0)} \in \mathcal{L}$ such that:*

- (a_1) $x_{i+1} \equiv x_i \bmod S\mathcal{N}^{(i+1)}$;
- (a_2) $V^{(i+1)}_{(b,m)} \equiv V^{(i)}_{(b,m)} \bmod \mathcal{L}(i+2)_k$;
- (a_3) $V^{(i+1)}_{(0)} \equiv V^{(i)}_{(0)} \bmod \mathcal{L}(i+2)$
- (b) *if* $e_i^\dagger = \sum_{b,m} S^{-m}t^b V^{(i)}_{(b,m)} + \alpha_0 V_0^{(i)}$ *then*

$$(-\sigma x_i) \circ e \circ x_i \equiv e_i^\dagger \bmod S\mathcal{N}^{(i+2)}.$$

Proof of Lemma 2.8. — Use the elements $V^{(0)}_{(b,m)}, V^{(0)}_{(0)}, e_0^\dagger$ and x_0 from the beginning of the proof of Proposition 2.6. Then part (b) holds for $i=0$ by (2.2).

Let $i_0 \geqslant 1$ and assume that our Lemma is proved for all $i < i_0$. Let $l \in S^{-i_0}\mathcal{L}(i_0+1)_{\mathrm{m}(\mathcal{K})}$ be such that

$$e^\dagger_{i_0-1} - (-\sigma x_{i_0-1}) \circ e \circ x_{i_0-1} \equiv l \bmod S\mathcal{N}^{(i_0+2)}.$$

Apply Lemma 2.7 to $\mathfrak{M} = \mathcal{L}(i_0+1)$ and $l \in S^{-i_0}\mathcal{L}(i_0+1)_{\mathrm{m}(\mathcal{K})}$. This gives us the appropriate elements $l_{(b,m)} \in \mathcal{L}(i_0+1)_k$, $l_{(0)} \in \mathcal{L}(i_0+1)$

and $\tilde{l} \in S^{-i_0}\mathcal{L}(i_0+1)_{\mathrm{m}(\mathcal{K})}$. Note that the elements $l_{(b,m)}$ are defined only for $1 \leqslant m \leqslant i_0$. Extend their definition by setting $l_{(b,m)} = 0$ if $m > i_0$. Then the case $i = i_0$ of Lemma 2.8 holds with $V_{(b,m)}^{(i_0)} = V_{(b,m)}^{(i_0-1)} + l_{(b,m)}$, $V_{(0)}^{(i_0)} = V_{(0)}^{(i_0-1)} + l_{(0)}$ and $x_{i_0} = x_{i_0-1} + \tilde{l}$. (We use here that $S\mathcal{N}^{(i_0+1)} = S^{-i_0}\mathcal{L}(i_0+1)_{\mathrm{m}(\mathcal{K})} + S\mathcal{N}^{(i_0+2)}$.)

Lemma 2.8 and Proposition 2.6 are completely proved. □

Proposition 2.6(b) implies that the elements $\sigma^n V_{(b,m)}$, $n \in \mathbb{Z}/N_0$, together with $V_{(0)}$ form a system of free topological generators of $\mathcal{L}_k$. Suppose $\{\beta_i\}_{1\leqslant i\leqslant N_0}$ and $\{\gamma_i\}_{1\leqslant i\leqslant N_0}$ are the $\mathbb{Z}/p^M$-bases of $W_M(k)$ from the proof of Proposition 1.2. Proceeding similarly to that proof introduce the elements

$$V_{(b,m),i} := \sum_{n\in\mathbb{Z}/N_0} \sigma^n(\beta_i)\sigma^n(V_{(b,m)})\,.$$

Then all $V_{(b,m)}$ can be recovered via the relation $V_{(b,m)} = \sum_i \gamma_i V_{(b,m),i}$. This implies that the elements $V_{(b,m),i}$ together with $V_{(0)}$ form a system of free topological generators of $\mathcal{L}$. (Recall that $\mathcal{L}$ is a free object in the category of Lie $\mathbb{Z}/p^M$-algebras of nilpotent class $< p$.) Therefore, we can introduce the weight function wt on $\mathcal{L}$ by setting for all b, m, i, $\mathrm{wt}(V_{(b,m),i}) = m$ and $\mathrm{wt}(V_{(0)}) = 1$. Note that by Proposition 2.6(b) we have that $e^\dagger \in \mathcal{N}$ if and only if $e \in \mathcal{N}$. Now Proposition 2.2 implies the following corollary.

Corollary 2.9. — *For any $s \geqslant 1$, $\mathcal{L}(s) = \{l \in \mathcal{L} \mid \mathrm{wt}(l) \geqslant s\}$.*

3. The groups $\widetilde{\mathcal{G}}_h$ and $\mathcal{G}_h$

3.1. Automorphism h

Let $S \in O(\mathcal{K})$ be the element introduced in Subsection 2.1. Let $h_0 \in \mathrm{Aut}(\mathcal{K})$ be such that $h_0|_k = \mathrm{id}$ and $h_0(t_0) = t_0E(1, S \bmod p)$. Then h_0 admits a lift to $h \in \mathrm{Aut}\, O(\mathcal{K})$ such that $h|_{W_M(k)} = \mathrm{id}$ and $h(t) = tE(1, S)$. Recall that $O(\mathcal{K}) = W_M(k)((t))$. If $n \in \mathbb{N}$ then denote by $h^n(t)$ the n-th superposition of the formal power series $h(t)$.

Proposition 3.1. — *For any $n \in \mathbb{N}$, $h^n(t) \equiv tE(n, S) \bmod S^p\mathrm{m}(\mathcal{K})$*

Proof. — If $n = 1$ there is nothing to prove. Suppose proposition is proved for some $n \in \mathbb{N}$. Then

$$h^{n+1}(t) = h^n(h(t)) \equiv tE(1, S)E(n, S(h(t))) \bmod \mathrm{m}(\mathcal{K})S(h(t))^p.$$

Recall, cf. Subsection 2.2, that $S = \sum_{l\geqslant 1}\gamma_{l1}t^l$, where $\gamma_{l1}\in W_M(k)$ and $\gamma_{l1}l=0$. Let $l=l'p^a$ with $\gcd(l',p)=1$. Then $\gamma_{l1}\in p^{M-a}W_M(k)$.

With the above notation we have in $W_M(k)[\![t]\!]$,

$$E(1,S)^l = \exp(p^aS+\cdots+pS^{p^{a-1}})^{l'}E(1,S^{p^a})^{l'} \equiv 1 \bmod (p^a, S^p).$$

Therefore (use that $\gamma_{l1}p^a=0$),

$$S(h(t)) \equiv S(tE(1,S)) \equiv \sum_l \gamma_{l1}t^lE(1,S)^l \equiv \sum_l \gamma_{l1}t^l = S \bmod S^p\,,$$

and $h^{n+1}(t) \equiv tE(1,S)E(n,S) \equiv tE(n+1,S) \bmod \mathrm{m}(\mathcal{K})S^p$ (use that $S(h(t))^p\equiv 0 \bmod S^p$). □

3.2. Specification of lifts $h_{<p}$

Note that $h(t)=t\alpha^{p^{M-1}}$, where $\alpha = E(1,S_0)^p$, and therefore, h commutes with σ, cf. Remark in Subsection 1.1. Now suppose that $h_{<p,0}\in \mathrm{Aut}\,\mathcal{K}_{<p}$ is a lift of h_0. Then Proposition 1.1 provides us with a unique $h_{<p}\in \mathrm{Aut}\,O(\mathcal{K}_{<p})$ such that $h_{<p}|_{O(\mathcal{K})}=h$ and $h_{<p} \bmod p = h_{<p,0}$. Therefore, we can work with arbitrary lifts $h_{<p,0}$ of h_0 by working with the appropriate lifts $h_{<p}$ of h. Note that all such lifts $h_{<p}$ commute with σ.

A lift $h_{<p}$ of h can be specified by the formalism of nilpotent Artin–Schreier theory as follows.

- Define similarly to [1] the continuous $W_M(k)$-linear operators $\mathcal{R},\mathcal{S}: \mathcal{L}_{\mathcal{K}}\longrightarrow \mathcal{L}_{\mathcal{K}}$ as follows.
- Suppose $\alpha\in\mathcal{L}_k$.
- For $n>0$, set $\mathcal{R}(t^n\alpha)=0$ and $\mathcal{S}(t^n\alpha) = -\sum_{i\geqslant 0}\sigma^i(t^n\alpha)$.
- For $n=0$, set $\mathcal{R}(\alpha)=\alpha_0(\mathrm{id}_{\mathcal{L}}\otimes\mathrm{Tr})(\alpha)$, $\mathcal{S}(\alpha)=\sum_{0\leqslant j<i<N_0}\sigma^j\alpha_0\,\sigma^i\alpha$, where $\mathrm{Tr}: W_M(k)\longrightarrow W_M(k)$ is induced by the trace map in $k/\mathbb{F}_p$ and $\alpha_0\in W_M(k)$ with $\mathrm{Tr}\alpha_0=1$ was fixed in Subsection 1.4.
- For $n=-n_1p^m$, $\gcd(n_1,p)=1$, set $\mathcal{R}(t^n\alpha)=t^{-n_1}\sigma^{-m}\alpha$ and $\mathcal{S}(t^n\alpha)=\sum_{1\leqslant i\leqslant m}\sigma^{-i}(t^n\alpha)$.

Similarly to [1] we have the following lemma. (We use also the special case $\mathfrak{M}=\mathbb{Z}_p$ of Lemma 2.7.)

Lemma 3.2. — *For any $b\in\mathcal{L}_{\mathcal{K}}$,*

(a) *$b=\mathcal{R}(b)+(\sigma-\mathrm{id}_{\mathcal{L}_{\mathcal{K}}})\mathcal{S}(b)$;*

(b) *if $b=b_1+\sigma c-c$, where $b_1\in\sum_{a\in\mathbb{Z}^+(p)}t^{-a}\mathcal{L}_k+\alpha_0\mathcal{L}$ and $c\in\mathcal{L}_{\mathcal{K}}$ then $\mathcal{R}(b)=b_1$ and $c-\mathcal{S}(b)\in\mathcal{L}$;*

(c) *for any $n\geqslant 0$, $\mathcal{R}$ and $\mathcal{S}$ map $S^{-n}\mathcal{L}_{\mathrm{m}(\mathcal{K})}$ to itself.*

According to Subsection 1.6, for the lift $h_{<p} \in \mathrm{Aut}\, O(\mathcal{K}_{<p})$ of h (which is attached to the lift $h_{<p,0}$ of h_0), we have that

$$h_{<p}(f) = c \circ (A \otimes \mathrm{id}_{O(\mathcal{K}_{<p})}) f\,.$$

Here $c \in \mathcal{L}_{\mathcal{K}}$ and $A = \mathrm{Ad}\, h_{<p} \in \mathrm{Aut}\,\mathcal{L}$ (cf. Subsection 1.6 for the definition of $\mathrm{Ad}\, h_{<p}$). Similarly to [1] it can be proved that the correspondence $h_{<p} \mapsto (c, A)$ is a bijection between the set of all lifts $h_{<p}$ of h and all $(c, A) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\,\mathcal{L}$ such that

$$(\mathrm{id}_{\mathcal{L}} \otimes h)(e) \circ c = (\sigma c) \circ (A \otimes \mathrm{id}_{O(\mathcal{K})})(e)\,. \tag{3.1}$$

This allows us to specify a choice of $h_{<p}$ step by step proceeding from $h_{<p} \bmod C_s(\mathcal{L}_{\mathcal{K}_{<p}})$ to $h_{<p} \bmod C_{s+1}(\mathcal{L}_{\mathcal{K}_{<p}})$ where $1 \leqslant s < p$, as follows.

Suppose c and A are already chosen modulo s-th commutators, i.e. we chose $(c_s, A_s) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\,\mathcal{L}$ satisfying the relation (3.1) modulo $C_s(\mathcal{L}_{\mathcal{K}})$.

Then set $c_{s+1} = c_s + X$ and $A_{s+1} = A_s + \mathcal{A}$, where $X \in C_s(\mathcal{L}_{\mathcal{K}})$ and $\mathcal{A} \in \mathrm{Hom}(\mathcal{L}, C_s(\mathcal{L}))$. Then (3.1) implies that (here $\mathcal{A}_k = \mathcal{A} \otimes W_M(k)$)

$$\begin{aligned}\sigma X - X + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} \mathcal{A}_k(D_{a0})& \\ \equiv (\mathrm{id}_{\mathcal{L}} \otimes h) e \circ c_s - \sigma c_s \circ (A_s \otimes \mathrm{id}_{O(\mathcal{K})}) e \bmod C_{s+1}(\mathcal{L}_{\mathcal{K}})&\end{aligned} \tag{3.2}$$

Now we can specify c_{s+1} and A_{s+1} by setting $X = \mathcal{S}(B_s)$ and $\sum_{a \in \mathbb{Z}^0(p)} t^{-a} \mathcal{A}_k(D_{a0}) = \mathcal{R}(B_s)$, where B_s is the right-hand side of the above recurrent relation. Note that the knowledge of all $\mathcal{A}_k(D_{a0})$ recovers uniquely the values of $\mathcal{A}$ on generators of $\mathcal{L}$ and gives well-defined $A_{s+1} \in \mathrm{Aut}\,\mathcal{L}$. Clearly, (c_{s+1}, A_{s+1}) satisfies the relation (3.1) modulo $C_{s+1}(\mathcal{L}_{\mathcal{K}})$. Finally, we obtain the solution $(c^0, A^0) := (c_p, A_p)$ of (3.1) and can use it to specify uniquely the lift $h^0_{<p}$ of h.

3.3. The group $\widetilde{\mathcal{G}}_h$

Consider the group of all continuous automorphisms of $\mathcal{K}_{<p}$ such that their restriction to $\mathcal{K}$ belongs to the closed subgroup in $\mathrm{Aut}\,\mathcal{K}$ generated by h_0. These automorphisms admit unique lifts to automorphisms of $O(\mathcal{K}_{<p})$ such that their restriction to $O(\mathcal{K})$ belongs to the subgroup $\langle h \rangle$ of $\mathrm{Aut}\, O(\mathcal{K})$ generated by h, cf. the beginning of Subsection 3.2. Denote the group of these lifts by $\widetilde{\mathcal{G}}_h$.

Use the identification η_M from Subsection 1.4 to obtain a natural short exact sequence of profinite p-groups

$$1 \longrightarrow G(\mathcal{L}) \longrightarrow \widetilde{\mathcal{G}}_h \longrightarrow \langle h \rangle \longrightarrow 1 \tag{3.3}$$

For any $s\geqslant 2$, the s-th commutator subgroup $C_s(\widetilde{\mathcal{G}}_h)$ is a normal subgroup in $G(\mathcal{L})$. Therefore, $\mathcal{L}_h(s):=C_s(\widetilde{\mathcal{G}}_h)$ is a Lie subalgebra of $\mathcal{L}$. Set $\mathcal{L}_h(1)=\mathcal{L}$. Clearly, for any $s_1,s_2\geqslant 1$, $[\mathcal{L}_h(s_1),\mathcal{L}_h(s_2)]\subset\mathcal{L}_h(s_1+s_2)$, in other words, the filtration $\{\mathcal{L}_h(s)\}_{s\geqslant 1}$ is central.

Theorem 3.3. — *For all $s\in\mathbb{N}$, $\mathcal{L}_h(s)=\mathcal{L}(s)$.*

Proof. — Use the notation from Subsection 2.5. Obviously, we have:

- $\mathcal{L}(s+1)=(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}+\mathcal{L}(s+1)\cap C_2(\mathcal{L})$, where the $W_M(k)$-module $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}$ is generated by all $V_{(b,m)}$ with $m\geqslant s+1$ (for the definition of $V_{(b.m)}$ cf. Proposition 2.6) and $\mathcal{L}(s+1)\cap C_2(\mathcal{L})=\sum_{s_1+s_2=s+1}[\mathcal{L}(s_1),\mathcal{L}(s_2)]$;
- $\mathcal{L}_h(s+1)$ is the ideal in $\mathcal{L}$ generated by $[\mathcal{L}_h(s),\mathcal{L}]$ and all elements of the form $(\mathrm{Ad}h_{<p})l\circ(-l)$, where $l\in\mathcal{L}_h(s)$ and $h_{<p}$ is a lift of h.

Consider the elements $V_{(0)}$ and $V_{(b,m),i}$ introduced in the end of Section 2). Recall that $m\in\mathbb{N}$, $1\leqslant b<e^*$ and $\gcd(b,p)=1$.

Lemma 3.4. — *There is a lift $h^1_{<p}$ such that if $(\mathrm{Ad}h^1_{<p})V_{(0)}=\widetilde{V}_{(0)}$ and for all b,m,i, $(\mathrm{Ad}h^1_{<p})V_{(b,m),i}=\widetilde{V}_{(b,m),i}$ then*

(a) $\widetilde{V}_{(0)}\equiv V_{(0)}\bmod C_2(\mathcal{L})$;
(b) $\widetilde{V}_{(b,m),i}\equiv V_{(b,m),i}+bV_{(b,m+1),i}\bmod(\mathcal{L}(m+2)+\mathcal{L}(m+1)\cap C_2(\mathcal{L}))$.

We shall prove this Lemma below.

Note the following immediate applications of this lemma:

(a) if $l\in\mathcal{L}(s)$ then $(\mathrm{Ad}h^1_{<p})l\circ(-l)\in\mathcal{L}(s+1)$;
(b) if $l\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s+1)}$ then there is an $l'\in(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s)}$ such that $(\mathrm{Ad}h^1_{<p})l'\circ(-l')\equiv l\bmod\mathcal{L}(s+1)\cap C_2(\mathcal{L})$.

Now we can finish the proof of our theorem.

Clearly, $\mathcal{L}_h(1)=\mathcal{L}(1)$.

Suppose $s_0\geqslant 1$ and for $1\leqslant s\leqslant s_0$, we have $\mathcal{L}_h(s)=\mathcal{L}(s)$.

Then $[\mathcal{L}_h(s_0),\mathcal{L}]=[\mathcal{L}(s_0),\mathcal{L}(1)]\subset\mathcal{L}(s_0+1)$ and applying (a) we obtain that $\mathcal{L}_h(s_0+1)\subset\mathcal{L}(s_0+1)$.

In the opposite direction, note that by inductive assumption,

$$\mathcal{L}(s_0+1)\cap C_2(\mathcal{L})=\sum_{s_1+s_2=s_0+1}[\mathcal{L}_h(s_1),\mathcal{L}_h(s_2)]\subset\mathcal{L}_h(s_0+1)$$

and then from (b) we obtain that $(\mathcal{K}^*/\mathcal{K}^{*p^M})^{(s_0+1)}\subset\mathcal{L}_h(s_0+1)$. So, $\mathcal{L}(s_0+1)\subset\mathcal{L}_h(s_0+1)$. The theorem is completely proved. □

Proof of Lemma 3.4. — Let

$$\tilde{e}^{\dagger} := (\mathrm{Ad}h^1_{<p} \otimes \mathrm{id}_{O(\mathcal{K})})e^{\dagger} = \sum_{i,b,m} \frac{t^b}{S^m}\beta_i \widetilde{V}_{(b,m),i} + \alpha_{(0)}\widetilde{V}_{(0)}\,.$$

Similarly to Subsection 3.2 there is $c^1 \in \mathcal{L}_{\mathcal{K}}$ such that

$$(\mathrm{id}_{\mathcal{L}} \otimes h)e^{\dagger} \circ c^1 = (\sigma c^1) \circ \tilde{e}^{\dagger}\,, \tag{3.4}$$

and the choice of $h^1_{<p}$ can be specified by an analog of the recurrent procedure from the end of Subsection 3.2.

Namely, set $c^1_1 = 0$ and $A^1_1 = \mathrm{id}_{\mathcal{L}}$. Then for $1 \leqslant s < p$, (c^1_{s+1}, A^1_{s+1}) can be defined as follows:

- $B_s = (\mathrm{id}_{\mathcal{L}} \otimes h)e^{\dagger} \circ c^1_s - (\sigma c^1_s) \circ (A^1_s \otimes \mathrm{id}_{\mathcal{K}})e^{\dagger}$
- $X_s = \mathcal{S}(B_s)$, $(\mathcal{A}_s \otimes \mathrm{id}_{\mathcal{K}})e^{\dagger} = \mathcal{R}(B_s)$;
- $c^1_{s+1} = c^1_s + X_s$, $A^1_{s+1} = A^1_s + \mathcal{A}_s$

This gives the system of compatible on $1 \leqslant s \leqslant p$ solutions $(c^1_s, A^1_s) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\,\mathcal{L}$ of (3.4) modulo $C_s(\mathcal{L}_{\mathcal{K}})$ and $(c^1, A^1) := (c^1_p, A^1_p)$ defines $h^1_{<p}$.

Let

$$\widetilde{\mathcal{N}}^{(2)} := \sum_{i \geqslant 2} S^{-i}(\mathcal{L}(i) \cap C_2(\mathcal{L}))_{\mathrm{m}(\mathcal{K})} \subset \mathcal{N}^{(2)}\,.$$

Note that $[\mathcal{N}, \mathcal{N}] \subset \widetilde{\mathcal{N}}^{(2)}$. Consider the following properties.

(1) $(\mathrm{id}_{\mathcal{L}} \otimes h)(e^{\dagger}) = e^{\dagger} + e^+_1 + e^-_1 \bmod S^2\mathcal{N}$, where $e^+_1, e^-_1 \in S\mathcal{N}$ and

$$e^-_1 = \sum_{i,b,m} \frac{bt^b}{S^m}\beta_i V_{(b,m+1),i}, \quad e^+_1 = \sum_{b,i} bt^b \beta_i V_{(b,1),i}$$

(use that $h(S) \equiv S(h(t)) \equiv S \bmod S^p$, cf. the proof of Proposition 3.1).

(2) $\tilde{e}^{\dagger} \equiv e^{\dagger} \bmod S\mathcal{N}$ and $c^1 \in S\mathcal{N}$ (use that for all s, $B_s \in S\mathcal{N}$ and $\mathcal{R}$ and $\mathcal{S}$ map $S\mathcal{N}$ to itself).

(3) $(-\sigma c^1) \circ (\mathrm{id}_{\mathcal{L}} \otimes h)(e^{\dagger}) \circ c^1 \equiv (c^1 - \sigma c^1) + e^{\dagger} + e^{\dagger}_1 \bmod S^2\mathcal{N} + S\widetilde{\mathcal{N}}^{(2)}$ (use that $c \in S\mathcal{N}$ and $(\mathrm{id}_{\mathcal{L}} \otimes h)(e^{\dagger}) \in \mathcal{N}$)

(4) Apply $\mathcal{R}$ to the congruence from c), use that $S^2\mathcal{N} + S\widetilde{\mathcal{N}}^{(2)}$ is mapped by $\mathcal{R}$ to itself and $\mathcal{R}(c^1 - \sigma c^1) = \mathcal{R}(e^+_1) = 0$

$$\tilde{e}^{\dagger} \equiv \sum_{i,b,m} \frac{t^b}{S^m}\beta_i \left(V_{(b,m),i} + bV_{(b,m+1),i}\right) + \alpha_0 V_{(0)} \bmod S^2\mathcal{N} + S\widetilde{\mathcal{N}}^{(2)}\,.$$

It remains to note that the last congruence is equivalent to the statement of our lemma. ∎

3.4. The group $\mathcal{G}_h$

Let $\mathcal{G}_h = \widetilde{\mathcal{G}}_h/\widetilde{\mathcal{G}}_h^{p^M} C_p(\widetilde{\mathcal{G}}_h)$.

Proposition 3.5. — *Exact sequence* (3.3) *induces the following exact sequence of p-groups*

$$1 \longrightarrow G(\mathcal{L})/G(\mathcal{L}(p)) \longrightarrow \mathcal{G}_h \longrightarrow \langle h\rangle \bmod \langle h^{p^M}\rangle \longrightarrow 1 \tag{3.5}$$

Proof. — Set

$$\mathcal{M} := \mathcal{N} + \mathcal{L}(p)_{\mathcal{K}} = \sum_{1\leqslant s<p} S^{-s}\mathcal{L}(s)_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(p)_{\mathcal{K}}$$

$$\mathcal{M}_{<p} := \sum_{1\leqslant s<p} S^{-s}\mathcal{L}(s)_{\mathrm{m}(\mathcal{K}_{<p})} + \mathcal{L}(p)_{\mathcal{K}_{<p}}$$

where $\mathrm{m}(\mathcal{K}_{<p}) = W_M(\mathrm{m}_{<p})\cap O(\mathcal{K}_{<p})$ and $\mathrm{m}_{<p}$ is the maximal ideal of the valuation ring of $\mathcal{K}_{<p}$.

Then $\mathcal{M}$ has the induced structure of Lie $W_M(k)$-algebra (use the Lie bracket from $\mathcal{L}_{\mathcal{K}}$) and $S^{p-1}\mathcal{M}$ is an ideal in $\mathcal{M}$. Similarly, $\mathcal{M}_{<p}$ is a Lie $W_M(k)$-algebra (containing $\mathcal{M}$ as its subalgebra) and $S^{p-1}\mathcal{M}_{<p}$ is an ideal in $\mathcal{M}_{<p}$. Note that $e\in\mathcal{M}$, $f\in\mathcal{M}_{<p}$, $S^{p-1}\mathcal{M}_{<p}\cap\mathcal{M} = S^{p-1}\mathcal{M}$, and we have a natural embedding of $\bar{\mathcal{M}} := \mathcal{M}/S^{p-1}\mathcal{M}$ into $\bar{\mathcal{M}}_{<p} := \mathcal{M}_{<p}/S^{p-1}\mathcal{M}_{<p}$. For $i\geqslant 0$, we have also $(\mathrm{id}_{\mathcal{L}}\otimes h - \mathrm{id}_{\mathcal{M}})^i\mathcal{M}\subset S^i\mathcal{M}$.

Consider the orbit of $\bar f := f \bmod S^{p-1}\mathcal{M}_{<p}$ with respect to the natural action of $\widetilde{\mathcal{G}}_h\subset \operatorname{Aut} O(\mathcal{K}_{<p})$ on $\bar{\mathcal{M}}_{<p}$. Prove that the stabilizer $\mathcal{H}$ of $\bar f$ equals $\widetilde{\mathcal{G}}_h^{p^M} C_p(\widetilde{\mathcal{G}}_h)$.

If $l\in G(\mathcal{L})$ then $\eta_M^{-1}(l)\in\mathcal{G}_{<p}$ sends f to $f\circ l$. This means that for $l\in\mathcal{L}\cap\mathcal{H}$ we have

$$l\in S^{p-1}\mathcal{M}_{<p}\cap\mathcal{L} = S^{p-1}\mathcal{M}\cap\mathcal{L} = \mathcal{L}(p)_{\mathcal{K}}\cap\mathcal{L} = \mathcal{L}(p) = C_p(\widetilde{\mathcal{G}}_h)\,.$$

Therefore, $\mathcal{H}\cap G(\mathcal{L}) = C_p(\widetilde{\mathcal{G}}_h)\subset\mathcal{H}$ and we obtain the embedding

$$\kappa : G(\mathcal{L})/G(\mathcal{L}(p)) \longrightarrow \widetilde{\mathcal{G}}_h/\mathcal{H}\,.$$

Now consider the lift $h^0_{<p}$ from the end of Subsection 3.2.

Note that $\widetilde{\mathcal{G}}_h^{p^M} \bmod C_p(\widetilde{\mathcal{G}}_h)$ is generated by $h^{0p^M}_{<p}$. Indeed, any finite p-group of nilpotent class $<p$ is P-regular, cf. [10] Subsection 12.3. In particular, for any $g\in G(\mathcal{L})$, $(h^0_{<p}\circ g)^{p^M}\equiv h^{0p^M}_{<p}\circ g' \bmod C_p(\widetilde{\mathcal{G}}_h)$, where g' is the product of p^M-th powers of elements from $G(\mathcal{L})$, but $G(\mathcal{L})$ has period p^M.

As earlier, $h^0_{<p}f = c^0\circ(A^0\otimes\mathrm{id}_{\mathcal{K}})f$. Note that $c^0\in S\mathcal{M}$ (proceed similarly to the proof of Lemma 3.4(b)).

Then

$$h^{0p^M}_{<p}(f)$$
$$= (\mathrm{id}\otimes h)^{p^M-1}\left(c^0\circ(A^0\otimes h^{-1})c^0\circ\dots\circ(A^0\otimes h^{-1})^{p^M-1}c^0\right)$$
$$\circ\,(A^{0p^M}\otimes\mathrm{id})f\,.$$

Clearly, $(A^0-\mathrm{id}_{\mathcal{L}})^p\mathcal{L}\subset\mathcal{L}(p)$ and, therefore, $(A^{0p^M}\otimes\mathrm{id})\bar f=\bar f$.

Similarly, $B=A^0\otimes h^{-1}$ is an automorphism of the Lie algebra $\mathcal{M}$, and for all $s\geqslant 0$, $(B-\mathrm{id}_{\mathcal{M}})(S^s\mathcal{M})\subset S^{s+1}\mathcal{M}$.

Lemma 3.6. — *For any $m\in\mathcal{SM}$, $m\circ B(m)\circ\dots\circ B^{p^M-1}m\in\mathcal{S}^p\mathcal{M}$.*

Proof. — Consider the Lie algebra $\mathfrak{M}=\mathcal{SM}/\mathcal{S}^p\mathcal{M}$ with the filtration $\{\mathfrak{M}(i)\}_{i\geqslant 1}$ induced by the filtration $\{S^i\mathcal{M}\}_{i\geqslant 1}$. This filtration is central, i.e. for any $i,j\geqslant 1$, $[\mathfrak{M}(i),\mathfrak{M}(j)]\subset\mathfrak{M}(i+j)$. In particular, the nilpotent class of $\mathfrak{M}$ is $<p$.

The operator B induces the operator on $\mathfrak{M}$ which we denote also by B. Clearly, $B=\widetilde{\exp}\,\mathcal{B}$ where $\mathcal{B}$ is a differentiation on $\mathfrak{M}$ such that for all $i\geqslant 1$, $\mathcal{B}(\mathfrak{M}(i))\subset\mathfrak{M}(i+1)$.

Let $\widetilde{\mathfrak{M}}$ be a semi-direct product of $\mathfrak{M}$ and the trivial Lie algebra $(\mathbb{Z}/p^M)w$ via $\mathcal{B}$. This means that $\widetilde{\mathfrak{M}}=\mathfrak{M}\oplus(\mathbb{Z}/p^M)w$ as $\mathbb{Z}/p^M$-module, $\mathfrak{M}$ and $(\mathbb{Z}/p^M)w$ are Lie subalgebras of $\widetilde{\mathfrak{M}}$ and for any $m\in\mathfrak{M}$, $[m,w]=\mathcal{B}(m)$. Clearly, $C_2(\widetilde{\mathfrak{M}})=[\widetilde{\mathfrak{M}},\widetilde{\mathfrak{M}}]\subset\mathfrak{M}(2)$. This implies that $\widetilde{\mathfrak{M}}$ has nilpotent class $<p$ and we can consider the p-group $G(\widetilde{\mathfrak{M}})$. This group has nilpotent class $<p$ and period p^M (because for any $\bar m\in\widetilde{\mathfrak{M}}$, its p^M-th power in $G(\widetilde{\mathfrak{M}})$ equals $p^M\bar m=0$).

Note that the conjugation by w in $G(\widetilde{\mathfrak{M}})$ is given by the automorphism $\widetilde{\exp}\,\mathcal{B}=B$. Indeed, if $m\in\mathfrak{M}$ then

$$B(m)=(\widetilde{\exp}\mathcal{B})m=\sum_{0\leqslant n<p}\mathcal{B}^n(m)/n!=(-w)\circ m\circ w$$

(use very well-known formula in a free associative algebra $\mathbb{Q}[\![X,Y]\!]$,

$$\exp(-Y)\exp(X)\exp(Y)=\exp(X+\ldots+(\mathrm{ad}^{\,n}Y)X/n!+\ldots)\,,$$

where $\mathrm{ad}\,Y: X\mapsto[X,Y]$).

In particular, for any element $\bar m=m\,\mathrm{mod}\,\mathcal{N}(p)\in\mathfrak{M}$, we have $w_1\circ\bar m=B(\bar m)\circ w_1$, where $w_1=-w$. Therefore, $0=(\bar m\circ w_1)^{p^M}=\bar m\circ B(\bar m)\circ\dots\circ B^{p^M-1}(\bar m)\circ w_1^{p^M}$, and it remains to note that $w_1^{p^M}=0$. □

Applying the above Lemma we obtain that

$$c^0\circ(A^0\otimes h^{-1})c^0\circ\dots\circ(A^0\otimes h^{-1})^{p^M-1}c^0\in\mathcal{N}(p)\subset S^{p-1}\mathcal{M}$$

and, therefore, $h_{<p}^{0p^M}(\bar{f}) = 0$.

Thus, we proved that $\widetilde{\mathcal{G}}_h^{p^M} C_p(\widetilde{\mathcal{G}}_h) \subset \mathcal{H}$.

Suppose $g = h_{<p}^m l \in \mathcal{H}$ with some $l \in G(\mathcal{L})$. Then $g(f) = b \circ f$ where $b \in S^{p-1}\mathcal{M}_{<p}$. Note that $\sigma(b) \in S^{p-1}\mathcal{M}_{<p}$. Then

$$g(e) \circ b \circ f = g(e) \circ g(f) = g(\sigma f) = \sigma b \circ \sigma f = \sigma b \circ e \circ f$$

implies that $g(e) \equiv e \operatorname{mod} S^{p-1}\mathcal{M}$. Thus $(\mathrm{id} \otimes h)^m(e) \equiv e \operatorname{mod} S^{p-1}\mathcal{M}$.

Now use that $e \equiv e^{\dagger} \operatorname{mod} \mathcal{L}_{\mathrm{m}(\mathcal{K})} + C_2(\mathcal{L})_{\mathcal{K}}$, cf. the beginning of the proof of Proposition 2.6.

Clearly, $\mathcal{L}_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(p)_{\mathcal{K}} \supset S^{p-1}\mathcal{M}$ and, therefore, for the element

$$e^{\dagger}_{<p} := \sum_{i,b} \sum_{1 \leqslant m < p} \frac{t^b}{S^m} \beta_i V_{(b,m),i}$$

we obtain $(\mathrm{id}_{\mathcal{L}} \otimes h)^m(e^{\dagger}_{<p}) \equiv e^{\dagger}_{<p} \operatorname{mod} \mathcal{L}_{\mathrm{m}(\mathcal{K})} + C_2(\mathcal{L}_{\mathcal{K}})$. But

$$h^m(e^{\dagger}_{<p}) \equiv \sum_{i,b} \sum_{1 \leqslant m < p} \frac{t^b E(bm, S)}{S^m} \beta_i V_{(b,m),i} \operatorname{mod} \mathcal{L}_{\mathrm{m}(\mathcal{K})} + \mathcal{L}(p)_{\mathcal{K}}$$

Now following the coefficients for $V_{(b,p-2),i}$ we obtain $m \equiv 0 \operatorname{mod} p^M$. Therefore, $l \in \mathcal{H} \cap G(\mathcal{L}) = C_p(\widetilde{\mathcal{G}}_h)$ and $\mathcal{H} \subset \widetilde{\mathcal{G}}_h^{p^M} C_p(\widetilde{\mathcal{G}}_h)$.

Finally, we have $\widetilde{\mathcal{G}}_h/\mathcal{H} = \mathcal{G}_h$, $\mathcal{H} \operatorname{mod} C_p(\widetilde{\mathcal{G}}_h) = \langle h_{<p}^{p^M} \rangle$ and, therefore, $\operatorname{Coker} \kappa = \langle h \rangle \operatorname{mod} \langle h^{p^M} \rangle$. □

Corollary 3.7. — *If L_h is a Lie $\mathbb{Z}/p^M$ algebra such that $\mathcal{G}_h = G(L_h)$ then* (3.5) *induces the following short exact sequence of Lie $\mathbb{Z}/p^M$-algebras*

$$0 \longrightarrow \mathcal{L}/\mathcal{L}(p) \longrightarrow L_h \longrightarrow (\mathbb{Z}/p^M)h \longrightarrow 0$$

Remark. — In [1] we studied the structure of the above Lie algebra L_h in the case $M = 1$. The case of arbitrary M will be considered in a forthcoming paper.

3.5. Ramification estimates

Use the identification from Subsection 1.3, $\eta_M : \mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K}) = \mathcal{G}_{<p} \simeq G(\mathcal{L})$ and set for all for $s \in \mathbb{N}$, $\mathcal{K}[s, M] := \mathcal{K}_{<p}^{G(\mathcal{L}(s+1))}$. Denote by $v(s, M)$ the maximal upper ramification number of the extension $\mathcal{K}[s, M]/\mathcal{K}$. In other words,

$$v(s, M) = \max\{v \mid \mathcal{G}_{<p}^{(v)} \text{ acts non-trivially on } \mathcal{K}[s, M]\}\,.$$

Proposition 3.8. — *For all $s \in \mathbb{N}$, $v(s,M) = p^{M-1}(e^*s-1)$ (for the definition of e^* cf, Subsection 2.1).*

Proof. — Recall, cf. Subsection 1.7, that for any $v \geqslant 0$, the ramification subgroups $\mathcal{G}^{(v)}_{<p}$ are identified with the ideals $\mathcal{L}^{(v)}$ of $\mathcal{L}$, and for sufficiently large $N = N(v)$, the ideal $\mathcal{L}^{(v)}_k$ is generated by all $\sigma^n\mathcal{F}^0_{\gamma,-N}$, where $\gamma \geqslant v$, $n \in \mathbb{Z}/N_0$ and the elements $\mathcal{F}^0_{\gamma,-N}$ are given by (1.3).

Let $e^0 = e^*(1-1/p)$.

Lemma 3.9. — *If $a \in \mathbb{Z}^+(p)$, $u \in \mathbb{N}$ and $0 \leqslant c < M$ then the following two conditions are equivalent:*

(a) $t^aS^{-u} \in \mathrm{m}(\mathcal{K}) \operatorname{mod} p^c\, O(\mathcal{K})$;

(b) $a > e^*u + e^0(c-1)$.

Proof of Lemma 3.9. — Proposition 2.1(c) implies that

$$t^aS^{-u} = t^{a-ue^*}\eta_0\left(1 + \sum_{i\geqslant 1} t^{-ie^0}\eta_i(u)p^i\right)$$

where η_0 and all $\eta_i(u)$ are invertible elements of $W_M(k)[\![t]\!] \subset O(\mathcal{K})$. Therefore, $t^aS^{-u} \in \mathrm{m}(\mathcal{K}) \operatorname{mod} p^cO(\mathcal{K})$ if and only if for all $1 \leqslant i < c$, $t^{a-ue^*-ie^0} \in \mathrm{m}(\mathcal{K})$, i.e. $a - ue^* - (c-1)e^0 > 0$. The lemma is proved. □

Corollary 3.10. — *$D_{an} \in \mathcal{L}(u)_k \operatorname{mod} p^cO(\mathcal{K})$ if and only if we have that $a \geqslant e^*(u-1) + (c-1)e^0 + 1$.*

Lemma 3.11. — *Suppose $N \geqslant 0$.*

(a) *If $\gamma > p^{M-1}(e^*s-1)$ then $\mathcal{F}^0_{\gamma,-N} \in \mathcal{L}(s+1)_k$;*

(b) *if $\gamma = p^{M-1}(e^*s-1)$ then*

$$\mathcal{F}^0_{\gamma,-N} \equiv p^{M-1}D_{e^*s-1,M-1} \operatorname{mod} \mathcal{L}(s+1)_k\,.$$

Proof of Lemma 3.11. — For any $\gamma > 0$, $\mathcal{F}^0_{\gamma,-N}$ is a $\mathbb{Z}/p^M$-linear combination of the monomials of the form

$$X(b\,;a_1,\dots,a_r;m_2,\dots,m_r) = p^ba_1[\dots[D_{a_1,b-m_1},D_{a_2,b-m_2}],\dots,D_{a_r,b-m_r}]\,,$$

where $0 \leqslant b < M$, $1 \leqslant r < p$, all $a_i \in \mathbb{Z}^0(p)$, $0 = m_1 \leqslant m_2 \leqslant \dots \leqslant m_r$, and

$$p^b\left(a_1 + \frac{a_2}{p^{m_2}} + \dots + \frac{a_r}{p^{m_r}}\right) = \gamma\,.$$

For $1 \leqslant i \leqslant r$, let $u_i \in \mathbb{Z}$ be such that (note that $p^M|e^*$, $p^{M-1}|e^0$ and if $M=1$ then $M-b-1=0$)

$$1 + e^*(u_i-1) + e^0(M-b-1) \leqslant a_i < e^*u_i + e^0(M-b-1)\,.$$

This means that all $D_{a_i,b-m_i}\in\mathcal{L}(u_i)_k \bmod p^{M-b}\mathcal{L}_k$.

Suppose $X(b\,;a_1,\dots,a_r;m_2,\dots,m_r)\notin\mathcal{L}(s+1)_k$. This implies that $u_1+\dots+u_r\leqslant s$ and, therefore, $a_1+\dots+a_r\leqslant e^*s+re^0(M-b-1)-r$.

If $\gamma>p^{M-1}(e^*s-1)$ then $a_1+\dots+a_r>p^{M-b-1}(e^*s-1)$ and

$$e^*s+re^0(M-b-1)-r>p^{M-b-1}(e^*s-1).$$

Set $c=M-b-1$, then $0\leqslant c<M$ and

$$(p^c-1)(e^*s-1)\leqslant r(e^0c-1)\,.$$

If $c=0$ then $r\leqslant 0$, contradiction.

If $c\geqslant 1$ then (use that $r\leqslant p-1$ and $s\geqslant 1$)

$$(1+p+\dots+p^{c-1})(e^*-1)\leqslant e^0c-1\,.$$

But then $e^*=e^0(1+1/(p-1))\geqslant e^0+1$ implies that $1+p+\dots+p^{c-1}<c$. This contradiction proves (a).

Suppose $\gamma=p^{M-1}(e^*s-1)$. Then the expression for $\mathcal{F}^0_{\gamma,-N}$ contains the term $p^{M-1}D_{e^*s-1,M-1}$. Take (with above notation) any another monomial $X(b;a_1,\dots,a_r;m_2,\dots,m_r)$ from the expression of $\mathcal{F}^0_{\gamma,-N}$. Clearly, $r\geqslant 2$. As earlier, the assumption that this monomial does not belong to $\mathcal{L}(s+1)_k$ implies that

$$(p^c-1)(e^*s-1)\leqslant r(e^0c-1)+1\,.$$

If $c=0$ then $r\leqslant 1$, contradiction.

If $c\geqslant 1$ then again use that $r\leqslant p-1$ to obtain

$$(1+p+\dots+p^{c-1})(e^*s-1)\leqslant e^0c-1+1/(p-1)<e^0c$$

and note that the left-hand side of this inequality $>ce^0$ (use that $e^*s-1\geqslant e^*-1\geqslant e^0$). The contradiction. The lemma is completely proved. □

It remains to note that Lemma 3.11 implies that

$$\max\{v\mid\mathcal{L}^{(v)}\not\subset\mathcal{L}(s+1)\}=p^{M-1}(e^*s-1)\,.$$

Proposition 3.8 is completely proved. □

4. Applications to the mixed characteristic case

Let K be a finite field extension of $\mathbb{Q}_p$ with the residue field $k\simeq\mathbb{F}_{p^{N_0}}$ and the ramification index e_K. Let π_0 be a uniformising element in K. Denote by $\bar K$ an algebraic closure of K and set $\Gamma=\mathrm{Gal}(\bar K/K)$. Assume that K contains a primitive p^M-th root of unity ζ_M.

4.1. The subgroup $\widetilde{\Gamma}$

For $n\in\mathbb{N}$, choose $\pi_n\in\bar{K}$ such that $\pi_n^p=\pi_{n-1}$. Let $\widetilde{K}=\bigcup_{n\in\mathbb{N}}K(\pi_n)$, $\Gamma_{<p}:=\Gamma/\Gamma^{p^M}C_p(\Gamma)$ and $\widetilde{\Gamma}=\mathrm{Gal}(\bar{K}/\widetilde{K})$. Then $\widetilde{\Gamma}\subset\Gamma$ induces a continuous group homomorphism $i:\widetilde{\Gamma}\longrightarrow\Gamma_{<p}$.

We have $\mathrm{Gal}(K(\pi_M)/K)=\langle\tau_0\rangle^{\mathbb{Z}/p^M}$, where $\tau_0(\pi_M)=\pi_M\zeta_M$. Let $j:\Gamma_{<p}\longrightarrow\mathrm{Gal}(K(\pi_M)/K)$ be a natural epimorphism.

Proposition 4.1. — *The following sequence*

$$\widetilde{\Gamma}\xrightarrow{i}\Gamma_{<p}\xrightarrow{j}\langle\tau_0\rangle^{\mathbb{Z}/p^M}\longrightarrow 1$$

is exact.

Proof. — For $n>M$, let $\zeta_n\in\bar{K}$ be such that $\zeta_n^p=\zeta_{n-1}$.

Consider $\widetilde{K}'=\bigcup_{n\geqslant M}K(\pi_n,\zeta_n)$. Then $\widetilde{K}'/K$ is Galois with the Galois group $\Gamma_{\widetilde{K}'/K}=\langle\sigma,\tau\rangle$. Here for any $n\geqslant M$ and some $s_0\in\mathbb{Z}$, $\sigma\zeta_n=\zeta_n^{1+p^Ms_0}$, $\sigma\pi_n=\pi_n$, $\tau(\zeta_n)=\zeta_n$, $\tau\pi_n=\pi_n\zeta_n$ and $\sigma^{-1}\tau\sigma=\tau^{(1+p^Ms_0)^{-1}}$.

Therefore, $\Gamma_{\widetilde{K}'/K}^{p^M}=\langle\sigma^{p^M},\tau^{p^M}\rangle$ and for the subgroup of second commutators we have $C_2(\Gamma_{\widetilde{K}'/K})\subset\langle\tau^{p^M}\rangle\subset\Gamma_{\widetilde{K}'/K}^{p^M}$. This implies that

$$\Gamma_{\widetilde{K}'/K}^{p^M}C_p(\Gamma_{\widetilde{K}'/K})=\langle\sigma^{p^M},\tau^{p^M}\rangle$$

and for $\Gamma_{\widetilde{K}'/K}(M):=\Gamma_{\widetilde{K}'/K}/\Gamma_{\widetilde{K}'/K}^{p^M}C_p(\Gamma_{\widetilde{K}'/K})$, we obtain a natural exact sequence

$$\langle\sigma\rangle\longrightarrow\Gamma_{\widetilde{K}'/K}(M)\longrightarrow\langle\tau\rangle\bmod\langle\tau^{p^M}\rangle=\langle\tau_0\rangle^{\mathbb{Z}/p^M}\longrightarrow 1\,.$$

Note that $\Gamma_{\widetilde{K}'}$ together with a lift $\hat{\sigma}\in\widetilde{\Gamma}$ of σ generate $\widetilde{\Gamma}$. The above short exact sequence implies that $\mathrm{Ker}\left(\Gamma_{<p}\longrightarrow\langle\tau_0\rangle^{\mathbb{Z}/p^M}\right)$ is generated by $\hat{\sigma}$ and the image of $\Gamma_{\widetilde{K}'}$. So, this kernel coincides with the image of $\widetilde{\Gamma}$ in $\Gamma_{<p}$. $\square$

4.2. Special choice of S and S_0

Let R be Fontaine's ring. We have a natural embedding $k\subset R$ and an element $t_0=(\pi_n\bmod p)_{n\geqslant 0}\in R$. Then we can identify the field $k((t_0))$ with the field $\mathcal{K}$ from Sections 1-3. If $R_0=\mathrm{Frac}\,R$ then $\mathcal{K}$ is a closed subfield of R_0 and the theory of the field-of-norms functor identifies R_0 with the completion of the separable closure $\mathcal{K}_{sep}$ of $\mathcal{K}$ in R_0. Note that R is the valuation ring of R_0 and denote by m_R the maximal ideal of R.

This allows us to identify $\mathcal{G}=\mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$ with $\widetilde{\Gamma}\subset\Gamma\subset\mathrm{Aut}\,R_0$. This identification is compatible with the appropriate ramification filtrations. Namely, if $\varphi_{\widetilde{K}/K}$ is the Herbrand function of the (arithmetically profinite) field extension $\widetilde{K}/K$ then for any $v\geqslant 0$, $\mathcal{G}^{(v)}=\Gamma^{(v_1)}\cap\widetilde{\Gamma}$, where $v_1=\varphi_{\widetilde{K}/K}(v)$.

Let as earlier, $\mathcal{G}_{<p}=\mathcal{G}/\mathcal{G}^{p^M}C_p(\mathcal{G})$. Then the embedding $\mathcal{G}=\widetilde{\Gamma}\subset\Gamma$ induces a natural continuous morphism ι of the infinite group $\mathcal{G}_{<p}$ to the finite group $\Gamma_{<p}$. Therefore, by Proposition 4.1 we obtain the following exact sequence

$$\mathcal{G}_{<p}\xrightarrow{\iota}\Gamma_{<p}\xrightarrow{j}\langle\tau_0\rangle^{\mathbb{Z}/p^M}\longrightarrow 1\,. \tag{4.1}$$

Let $\zeta_M=1+\sum_{i\geqslant 1}[\beta_i]\pi_0^i$ with all $\beta_i\in k$. Consider the identification of rings $R/t_0^{e_K}\simeq O_{\bar{K}}/p$ given by $(r_0,\dots,r_n,\dots)\mapsto r_0$. If $\varepsilon=(\zeta_n)_{n\geqslant 0}$ is Fontaine's element such that ζ_M is our fixed p^M-th root of unity then we have in $W_M(R)$ the following congruence (as earlier, $t=(t_0,\dots,0)\in W_M(R)$)

$$\sigma^{-M}\varepsilon\equiv 1+\sum_{i\geqslant 1}\beta_i t^i \bmod (t^{e_K},p)\,. \tag{4.2}$$

Now we can specify the choice of the elements $S_0,S\in\mathrm{m}(\mathcal{K})$, cf. Subsection 2.1, by setting $E(1,S_0)=1+\sum_i\beta_i t^i$ and $S=[p]^M(S_0)$. Note that $S\bmod p$ generates the ideal $(t_0^{e^*})$ in $O_{\mathcal{K}}=k[\![t_0]\!]$, where $e^*=pe_K/(p-1)$. Now congruence (4.2) can be rewritten in the following form

$$\sigma^{-M}\varepsilon\equiv E(1,S_0)\bmod(\sigma^{-1}S^{p-1},p)\,.$$

Applying σ we obtain

$$\sigma^{-M+1}\varepsilon\equiv E(1,[p]S_0)\bmod(S^{p-1},p)\,,$$

and then taking p^{M-1}-th power

$$\varepsilon\equiv E(1,S)\bmod S^{p-1}W_M(R)\,.$$

4.3. The lifts $\eta_{<p}$

Let $v_{\mathcal{K}}$ be the extension of the normalized valuation on $\mathcal{K}$ to R_0. Consider a continuous field embedding $\eta_0:\mathcal{K}\longrightarrow R_0$ compatible with $v_{\mathcal{K}}$. Denote by $\mathrm{Iso}(\eta_0,\mathcal{K}_{<p},R_0)$ the set of all extensions $\eta_{<p,0}$ of η_0 to $\mathcal{K}_{<p}$. This set is a principal homogeneous space over $\mathcal{G}_{<p}=G(\mathcal{L})$.

Choose a lift $\eta : O(\mathcal{K}) \longrightarrow W_M(R_0)$ such that $\eta \bmod p = \eta_0$ and $\eta\sigma = \sigma\eta$. Proceeding similarly to Subsection 1.1 we can identify the set of all lifts $\eta_{0,<p}$ of η_0 from $\mathrm{Iso}(\eta_0, \mathcal{K}_{<p}, R_0)$ with the set of all (commuting with σ) lifts $\eta_{<p}$ of η from $\mathrm{Iso}(\eta, O(\mathcal{K}_{<p}), W_M(R_0))$.

Specify uniquely each lift $\eta_{<p}$ by the knowledge of $\eta_{<p}(f) \in \mathcal{L}_{R_0}$ in the set of all solutions $f' \in \mathcal{L}_{R_0}$ of the equation $\sigma f' = \eta(e) \circ f'$. (The elements $e \in \mathcal{L}_{\mathcal{K}}$ and $f \in \mathcal{L}_{\mathcal{K}_{<p}}$ were chosen in Subsection 1.4.)

Consider the appropriate submodules $\mathcal{M} \subset \mathcal{L}_{\mathcal{K}}$, $\mathcal{M}_{<p} \subset \mathcal{L}_{\mathcal{K}_{<p}}$ from Subsection 3.4 and define similarly

$$\mathcal{M}_{R_0} = \sum_{1 \leqslant s < p} S^{-s}\mathcal{L}(s)_{\mathrm{m}(R)} + \mathcal{L}(p)_{R_0} \subset \mathcal{L}_{R_0}\,,$$

where $\mathrm{m}(R) = W_M(\mathrm{m}_R)$. We know that $e \in \mathcal{M}$, $f \in \mathcal{M}_{<p}$ and for similar reasons, all $\eta_{<p}(f) \in \mathcal{M}_{R_0}$.

Lemma 4.2. — *With above notation suppose that*

$$\eta(e) \equiv e \bmod S^{p-1}\mathcal{M}_{R_0}.$$

Then there is $c \in S^{p-1}\mathcal{M}_{R_0}$ such that $\eta(e) = \sigma c \circ e \circ (-c)$.

Proof. — Note that $S^{p-1}\mathcal{M}_{R_0}$ is an ideal in $\mathcal{M}_{R_0}$ and for any $i \in \mathbb{N}$ and $m \in S^{p-1}C_i(\mathcal{M}_{R_0})$, there is $c \in S^{p-1}C_i(\mathcal{M}_{R_0})$ such that $\sigma c - c = m$. (Use that σ is topologically nilpotent on $S^{p-1}C_i(\mathcal{M}_{R_0})$.)

Therefore, there is $c_1 \in S^{p-1}\mathcal{M}_{R_0}$ such that $\eta(e) = e + \sigma c_1 - c_1$. This implies that $\eta(e) \circ c_1 \equiv \sigma c_1 \circ e \bmod S^{p-1}C_2(\mathcal{M}_{R_0})$. Similarly, there is $c_2 \in S^{p-1}C_2(\mathcal{M}_{R_0})$ such that $\eta(e) \circ c_1 + c_2 = \sigma c_2 + \sigma c_1 \circ e_0$ and $\eta(e_0) \circ c_1 \circ c_2 \equiv \sigma c_2 \circ \sigma c_1 \circ e_0 \bmod S^{p-1}C_3(\mathcal{M}_{R_0})$, and so on.

After $p-1$ iterations we obtain for $1 \leqslant i < p$ the elements $c_i \in S^{p-1}C_i(\mathcal{M}_{R_0})$ such that

$$\eta(e) \circ (c_1 \circ \cdots \circ c_{p-1}) = \sigma(c_{p-1} \circ \cdots \circ c_1) \circ e.$$

The lemma is proved. □

The above lemma implies the following properties:

Proposition 4.3.

(a) *If $\eta(e) \equiv e \bmod S^{p-1}\mathcal{M}_{R_0}$ then for any $\eta_{<p} \in \mathrm{Iso}(\eta, \mathcal{K}_{<p}, R_0)$, there is a unique $l \in G(\mathcal{L}) \bmod G(\mathcal{L}(p))$ such that*

$$\eta_{<p}(f) \equiv f \circ l \bmod S^{p-1}\mathcal{M}_{R_0}\,.$$

(b) *Suppose $\eta', \eta'' : O(\mathcal{K}) \longrightarrow W_M(R_0)$ are such that*

$$\eta'(t) \equiv \eta''(t) \bmod S^{p-1}W_M(\mathrm{m}_R)\,.$$

If $\eta'_{<p} \in \mathrm{Iso}(\eta', O(\mathcal{K}_{<p}), W_M(R_0))$ *and* $\eta''_{<p} \in \mathrm{Iso}(\eta'', O(\mathcal{K}_{<p}), W_M(R_0))$ *then there is a unique* $l \in G(\mathcal{L})$ *such that*

$$\eta'_{<p}(f) \equiv \eta''_{<p}(f) \circ l \bmod S^{p-1}\mathcal{M}_{R_0}.$$

4.4. Upper ramification numbers $v(K[s,M]/K)$

The action of $\Gamma = \mathrm{Gal}(\bar{K}/K)$ on R_0 is strict and, therefore, the elements $g \in \Gamma$ can be identified with all continuous field embeddings $g : \mathcal{K}_{sep} \to R_0$ such that $g|_{\mathcal{K}}$ belongs to the set $\langle \tau_0 \rangle = \{\tau_0^a \mid a \in \mathbb{Z}_p\}$.

Extend τ_0 now to a continuous embedding $\tau : O(\mathcal{K}) \longrightarrow W_M(R_0)$ uniquely determined by the condition $\tau(t) = t\varepsilon$. Clearly, τ commutes with σ. Then the results of Subsection 1.1 imply that the elements of Γ are identified with the continuous embeddings $g : O(\mathcal{K}_{sep}) \to W_M(R_0)$ such that $g|_{O(\mathcal{K})}$ belongs to the set $\langle \tau \rangle$.

Consider $h_0 \in \mathrm{Aut}(\mathcal{K})$ such that $h_0(t_0) = t_0 E(1, S \bmod p)$ and $h_0|_k = \mathrm{id}$. Then its lift $h \in \mathrm{Aut} O(\mathcal{K})$ such that $h(t) = tE(1,S)$ commutes with σ and there are the appropriate groups $\widetilde{\mathcal{G}}_h$ and $\mathcal{G}_h$ from Section 3.

Clearly, $h(t) \equiv \tau(t) \bmod S^{p-1}\mathrm{m}_R$ and we can apply Proposition 4.3(b). This implies that the Γ-orbit of $f \bmod S^{p-1}\mathcal{M}_{R_0}$ is contained in the $\widetilde{\mathcal{G}}_h$-orbit of $f \bmod S^{p-1}\mathcal{M}_{R_0}$. Therefore, there is a map of sets $\kappa : \Gamma \longrightarrow \mathcal{G}_h$ uniquely determined by the requirement that for any $g \in \Gamma$,

$$(\mathrm{id}_{\mathcal{L}} \otimes g) f \equiv (\mathrm{id}_{\mathcal{L}} \otimes \kappa(g)) f \bmod S^{p-1}\mathcal{M}_{R_0}\,.$$

(Use that $\mathcal{G}_h$ strictly acts on the $\widetilde{\mathcal{G}}_h$-orbit of $f \bmod S^{p-1}\mathcal{M}_{R_0}$.)

Proposition 4.4. — *κ induces a group isomorphism $\kappa_{<p} : \Gamma_{<p} \longrightarrow \mathcal{G}_h$.*

Proof. — Suppose $g_1, g \in \Gamma$. Let $c \in \mathcal{L}_{\mathcal{K}}$ and $A \in \mathrm{Aut}\,\mathcal{L}$ be such that $(\mathrm{id}_{\mathcal{L}} \otimes \kappa(g))f = c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$. Then we have the following congruences modulo $S^{p-1}\mathcal{M}_{R_0}$

$$\begin{aligned}
(\mathrm{id}_{\mathcal{L}} \otimes \kappa(g_1 g))f &\equiv (\mathrm{id}_{\mathcal{L}} \otimes g_1 g)f \equiv (\mathrm{id}_{\mathcal{L}} \otimes g_1)(\mathrm{id}_{\mathcal{L}} \otimes g)f \\
&\equiv (\mathrm{id}_{\mathcal{L}} \otimes g_1)(\mathrm{id}_{\mathcal{L}} \otimes \kappa(g))f \equiv (\mathrm{id}_{\mathcal{L}} \otimes g_1)(c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f) \\
&\equiv (\mathrm{id}_{\mathcal{L}} \otimes g_1)c \circ (A \otimes g_1)f \equiv (\mathrm{id}_{\mathcal{L}} \otimes \kappa(g_1))c \circ (A \otimes \kappa(g_1))f \\
&\equiv (\mathrm{id}_{\mathcal{L}} \otimes \kappa(g_1))(c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f) \equiv (\mathrm{id}_{\mathcal{L}} \otimes \kappa(g_1))(\mathrm{id}_{\mathcal{L}} \otimes \kappa(g))f \\
&\equiv (\mathrm{id}_{\mathcal{L}} \otimes \kappa(g_1)\kappa(g))f
\end{aligned}$$

and, therefore, $\kappa(g_1 g) = \kappa(g_1)\kappa(g)$ (use that $\mathcal{G}_h$ acts strictly on the orbit of f).

Therefore, κ factors through the natural projection $\Gamma \to \Gamma_{<p}$ and defines the group homomorphism $\kappa_{<p} : \Gamma_{<p} \to \mathcal{G}_h$.

Recall that we have the field-of-norms identification $\widetilde{\Gamma} = \mathcal{G}$ and, therefore, $\kappa_{<p}$ identifies the groups $\kappa(\widetilde{\Gamma})$ and $G(\mathcal{L}/\mathcal{L}(p)) \subset \mathcal{G}_h$. Besides, κ induces a group isomorphism of $\langle \tau_0 \rangle^{\mathbb{Z}/p^M}$ and $\langle h_0 \rangle^{\mathbb{Z}/p^M}$. Now Proposition 4.1 implies that $\kappa_{<p}$ is isomorphism. $\square$

Under the isomorphism $\kappa_{<p}$, the subfields $\mathcal{K}[s, M] \subset \mathcal{K}_{<p}$, where $1 \leqslant s < p$ (cf. Subsection 3.5), give rise to the subfields $K[s, M] \subset K_{<p}$ such that $\mathrm{Gal}(K[s, M]/K) = \Gamma/\Gamma^{p^M} C_{s+1}(\Gamma)$. In other words, the extensions $K[s, M]$ appear as the maximal p-extensions of K with the Galois group of period p^M and nilpotent class s.

Using that the identification $\mathcal{G} = \widetilde{\Gamma}$ is compatible with ramification filtrations, cf. Subsection 4.2, we obtain the following result about the maximal upper ramification numbers of the field extensions $K[s, M]/K$, where $M \in \mathbb{N}$ and $1 \leqslant s < p$.

Theorem 4.5. — *If $[K : \mathbb{Q}_p] < \infty$, e_K is the ramification index of K and $\zeta_M \in K$ then for $1 \leqslant s < p$,*

$$v(K[s, M]/K) = e_K \left(M + \frac{s}{p-1} \right) - \frac{1 - \delta_{1s}}{p} .$$

Proof. — Note first, that the Herbrand function $\varphi_{\widetilde{K}/K}(x)$ is continuous for all $x \geqslant 0$, $\varphi_{\widetilde{K}/K}(0) = 0$ and its derivative $\varphi'_{\widetilde{K}/K}$ equals 1 if $x \in (0, e^*)$ and equals p^{-m}, if $m \in \mathbb{N}$ and $x \in (e^* p^{m-1}, e^* p^m)$.

From Proposition 3.8 we obtain that

$$v(K[s, M]/K) = \max \left\{ v(K(\pi_M)/K), \varphi_{\widetilde{K}/K}(p^{M-1}(se^* - 1)) \right\} .$$

Note that $v(K(\pi_M)/K) = \varphi_{\widetilde{K}/K}(p^{M-1}e^*) = e^* + e_K(M-1)$ and, therefore,

$$v(K[1, M]/K) = v(K(\pi_M)/K) = e_K \left(M + \frac{1}{p-1} \right) .$$

If $2 \leqslant s < p$ then $v(K[s, M/K)$ equals

$$\begin{aligned} \varphi_{\widetilde{K}/K}(p^{M-1}(se^* - 1)) &= \varphi_{\widetilde{K}/K}(p^{M-1}e^*) + \frac{p^{M-1}(se^* - 1) - p^{M-1}e^*}{p^M} \\ &= e_K \left(M + \frac{s}{p-1} \right) - \frac{1}{p} . \end{aligned}$$

$\square$

BIBLIOGRAPHY

[1] V. Abrashkin, "Automorphisms of local fields of period p and nilpotent class $< p$", `http://arxiv.org/abs/1403.4121`.

[2] ———, "Ramification filtration of the Galois group of a local field", in *Proceedings of the St. Petersburg Mathematical Society III*, Amer. Math. Soc. Transl. Ser. 2, vol. 166, Am. Math. Soc., 1995, p. 35-100.

[3] ———, "Ramification filtration of the Galois group of a local field. II", *Proceedings of Steklov Math. Inst.* **208** (1995), p. 15-62.

[4] ———, "Ramification filtration of the Galois group of a local field. III", *Izv. Ross. Akad. Nauk, Ser. Mat.* **62** (1998), no. 5, p. 3-48, English transl. in *Izv. Math.* **62**, no. 5, p. 857-900.

[5] ———, "On a local analogue of the Grothendieck Conjecture", *Int. J. Math.* **11** (2000), no. 1, p. 3-43.

[6] ———, "Modified proof of a local analogue of the Grothendieck Conjecture", *J. Théor. Nombres Bordeaux* **22** (2010), no. 1, p. 1-50.

[7] ———, "Galois groups of local fields, Lie algebras and ramification", in *Arithmetic and Geometry*, London Mathematical Society Lecture Note Series, vol. 420, Cambridge University Press, 2015, p. 1-23.

[8] V. Abrashkin & R. Jenni, "The field-of-norms functor and the Hilbert symbol for higher local fields", *J. Théor. Nombres Bordeaux* **24** (2012), no. 1, p. 1-39.

[9] J.-M. Fontaine, "Représentations p-adiques des corps locaux. I.", in *The Grothendieck Festschrift, A Collection of Articles in Honor of the 60th Birthday of Alexander Grothendieck, vol. II*, Prog. Math., vol. 87, Birkhäuser, 1990, p. 249-309.

[10] M. j. Hall, *The theory of groups*, The Macmillan Company, 1959, xiii+434 pages.

[11] E. I. Khukhro, *p-automorphisms of finite p-groups*, London Mathematical Society Lecture Note Series, vol. 246, Cambridge University Press, 1998, xviii+204 pages.

[12] M. Lazard, "Sur les groupes nilpotents et les anneaux de Lie", *Ann. Sci. Éc. Norm. Supér.* **71** (1954), p. 101-190.

[13] S. Mochizuki, "A version of the Grothendieck conjecture for p-adic local fields", *Int. J. Math.* **8** (1997), no. 4, p. 499-506.

[14] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979, vii+241 pages.

[15] J.-P. Winterberger, "Le corps des normes de certaines extensions infinies des corps locaux; applications", *Ann. Sci. Éc. Norm. Supér.* **16** (1983), p. 59-89.

Manuscrit reçu le 22 juin 2015,
révisé le 23 mai 2016,
accepté le 14 juin 2016.

Victor ABRASHKIN
Department of Mathematical Sciences
Durham University
Lower Mountjoy, Stockton Rd
DH1 3LE (UK)
Steklov Institute
Gubkina str. 8
119991 Moscow (Russia)
victor.abrashkin@durham.ac.uk