# GROUPS OF AUTOMORPHISMS OF LOCAL FIELDS OF PERIOD $p$ AND NILPOTENT CLASS $< p$, I

VICTOR ABRASHKIN

Abstract. Suppose $K$ is a finite field extension of $\mathbb{Q}_p$ containing a primitive $p$-th root of unity. Let $K_{<p}$ be a maximal $p$-extension of $K$ with the Galois group of period $p$ and nilpotent class $< p$. In this paper we develop formalism which allows us to study the structure of $\Gamma_{<p} = Gal(K_{<p}/K)$ via methods of Lie theory. In particular, we introduce an explicit construction of a Lie $\mathbb{F}_p$-algebra $L$ and an identification $\Gamma_{<p} = G(L)$, where $G(L)$ is a $p$-group obtained from the elements of $L$ via the Campbell-Hausdorff composition law. In the next paper we apply this formalism to describe the ramification filtration $\{\Gamma_{<p}^{(v)}\}_{v \geqslant 0}$ and an explicit form of the Demushkin relation for $\Gamma_{<p}$.

## Introduction

Everywhere in the paper $p$ is a prime number, $p > 2$.

Let $K$ be a complete discrete valuation field with finite residue field $k \simeq \mathbb{F}_{p^{N_0}}$, $N_0 \in \mathbb{N}$. Let $K_{sep}$ be a separable closure of $K$ and $\Gamma = \mathrm{Gal}(K_{sep}/K)$.

A profinite group structure of $\Gamma$ is well-known, [11]. Most significant information about this structure comes from the maximal $p$-quotient $\Gamma(p)$ of $\Gamma$, [12, 18, 19]. As a matter of fact, the structure of $\Gamma(p)$ is not too complicated: its (topological) module of generators equals $K^*/K^{*p}$ and if $K$ has no non-trivial $p$-th roots of unity (e.g. if $\mathrm{char}K = p$) then $\Gamma(p)$ is pro-finite free; otherwise, $\Gamma(p)$ has finitely many generators and only one (the Demushkin) relation of a very special form.

In [1, 2, 3] the author introduced new techniques (nilpotent Artin-Schreier theory) which allowed us to study $p$-extensions of characteristic $p$ with Galois groups of nilpotent class $< p$. Such groups come from Lie algebras via classical equivalence $L \mapsto G(L)$ of the categories of Lie $\mathbb{F}_p$-algebras and $p$-groups of period $p$ of the same nilpotent class $s_0 < p$, [15]. This equivalence can be briefly explained as follows.

Suppose $\mathbb{Q}[[X, Y]]$ is a free associative algebra in two (non-commuting) variables $X$ and $Y$ with coefficients in $\mathbb{Q}$. Then the classical Campbell-Hausdorff formula

$$X \circ Y = \log(\exp(X) \cdot \exp(Y)) = X + Y + (1/2)[X, Y] + \dots$$

*Key words and phrases.* local field, Galois group, ramification filtration.

has $p$-integral coefficients modulo $p$-th commutators. If $L$ is a finite (resp., profinite) Lie $\mathbb{F}_p$-algebra of nilpotent class $< p$, we can introduce the finite (resp., profinite) group $G(L)$ which equals $L$ as a set and is provided with the Campbell-Hausdorff composition law $l_1 \circ l_2 = l_1 + l_2 + (1/2)[l_1, l_2] + \dots$. The correspondence $L \mapsto G(L)$ induces the above equivalence of categories. Under this equivalence any morphism of Lie algebras $L_1 \longrightarrow L$ is at the same time a group homomorphism $G(L_1) \longrightarrow G(L)$. In particular, $I$ is an ideal in $L$ iff $G(I)$ is a normal subgroup in $G(L)$; any $l_1, l_2 \in L$ are congruent modulo the ideal $I$ iff these elements (when considered as elements of the group $G(L)$) are congruent modulo the subgroup $G(I)$.

Suppose $K$ is a complete discrete valuation field of mixed characteristic containing a primitive $p$-th root of unity $\zeta_1$. Let $K_{<p}$ be the maximal $p$-extension of $K$ in $K_{sep}$ with Galois group of nilpotent class $< p$ and period $p$. Then $\Gamma_{<p} = \mathrm{Gal}(K_{<p}/K)$ has finitely many generators and one relation. (This terminology makes sense in the category of $p$-groups of nilpotent class $< p$ and period $p$.)

In this paper we use the nilpotent Artin-Schreier theory and the field-of-norms functor to obtain an explicit construction of a Lie $\mathbb{F}_p$-algebra $L$ and a group identification $\Gamma_{<p} = G(L)$. The group $G(L)$ starts reflecting all essential information about the field $K$ when provided with the filtration by the ramification subgroups $\Gamma_{<p}^{(v)} = G(L^{(v)})$, $v \geqslant 0$, cf. [16, 4, 5]. (Here $\Gamma_{<p}^{(v)}$ are the images of the ramification subgroups $\Gamma^{(v)}$ in $\Gamma$ and all $L^{(v)}$ are ideals in $L$.) In the second part [8] of this paper we describe the ramification filtration $L^{(v)}$, $v \geqslant 0$, and find an explicit form of the Demushkin relation in terms related to this filtration. Note that a similar technique ([7] and papers in progress) can be used to treat not only the similar quotients $\Gamma_{<p}(M)$ of $\Gamma$ of period $p^M$ but also the case of higher local fields $K$.

For the first approach to ramification filtration cf. [21], where the ramification filtration in $\Gamma^p C_2(\Gamma)/\Gamma^p C_3(\Gamma)$ was studied under some restrictions to the basic field $K$. The methods and techniques from [21] could not be applied to a more general situation. The principal advantage of our method is that we work with the whole group $\Gamma_{<p}$ rather than with the quotients of its central series.

### 0.1. **Main steps.**

*Notation.* If $G$ is a topological group and $s \in \mathbb{N}$ then $C_s(G)$ is the closure of the subgroup of commutators of order $\geqslant s$. With this notation, $G/G^p C_s(G)$ is the maximal quotient of $G$ of period $p$ and nilpotent class $< s$. Similarly, if $L$ is a topological Lie $\mathbb{F}_p$-algebra then $C_s(L)$ is the closure of the ideal of commutators of order $\geqslant s$ and $L/C_s(L)$ is the maximal quotient of nilpotent class $< s$. For any topological $\mathbb{F}_p$-module $\mathcal{M}$ we use the notation $L_{\mathcal{M}} = L\hat{\otimes}_{\mathbb{F}_p}\mathcal{M}$. In particular, if $\sigma$ is the Frobenius automorphism of $k \simeq \mathbb{F}_{p^{N_0}}$ then $\mathrm{id}_L \otimes \sigma$

acts on $L_k$. For simplicity, we denote $\mathrm{id}_L \otimes \sigma$ just by $\sigma$. Note that $L_k|_{\sigma=\mathrm{id}} = L$.

a) *Relation to the characteristic p case.*

Let $\pi_0$ be a fixed uniformizer in $K$ and $\widetilde{K} = K(\{\pi_n \mid n \in \mathbb{N}\})$, where $\pi_n^p = \pi_{n-1}$. If $X$ is the field-of-norms functor [20], then $X(\widetilde{K}) = \mathcal{K}$ is a complete discrete valuation field of characteristic $p$ with residue field $k$ and fixed uniformizer $t = \varprojlim \pi_n$. The functor $X$ induces identification of $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$ with $\Gamma_{\widetilde{K}} = \mathrm{Gal}(\bar{K}/\tilde{K})$. This gives us the following fundamental short exact sequence in the category of $p$-groups (where $\mathcal{G}_{<p} := \mathcal{G}/\mathcal{G}^p C_p(\mathcal{G})$ and $\tau_0(\pi_1) = \zeta_1\pi_1$)

$$\mathcal{G}_{<p} \xrightarrow{\iota_{<p}} \Gamma_{<p} \longrightarrow \mathrm{Gal}(K(\pi_1)/K) \left(= \langle\tau_0\rangle^{\mathbb{Z}/p}\right) \longrightarrow 1\,. \tag{0.1}$$

b) *Nilpotent Artin-Schreier theory.*

This theory allows us to fix an identification $\eta_0 : \mathcal{G}_{<p} \simeq G(\mathcal{L})$, where $\mathcal{L}$ is a profinite Lie $\mathbb{F}_p$-algebra. The identification $\eta_0$ depends on the uniformizer $t$ and a choice of $\alpha_0 \in k$ such that $\mathrm{Tr}_{k/\mathbb{F}_p}(\alpha_0) = 1$. Note that $\mathcal{L}_k$ appears with the system of generators

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

where $\mathbb{Z}^+(p) = \{a \in \mathbb{N} \mid \gcd(a,p) = 1\}$ and for any $a$, $\sigma(D_{an}) = D_{a,n+1}$. We will treat $D_0$ in the context of all $D_{an}$ by setting for all $n \in \mathbb{Z}/N_0$, $D_{0n} = (\sigma^n\alpha_0)D_0$.

c) *Ramification filtration in $\mathcal{G}_{<p}$.*

With respect to the above identification $\eta_0$ the ramification subgroups $\mathcal{G}_{<p}^{(v)}$ come from the ideals $\mathcal{L}^{(v)}$ of $\mathcal{L}$. In [1, 2, 3] we constructed explicitly the elements $\mathcal{F}^0_{\gamma,-N} \in \mathcal{L}_k$ with non-negative $\gamma \in \mathbb{Q}$ and $N \in \mathbb{Z}$, such that for any $v \geqslant 0$ and sufficiently large $N \geqslant \widetilde{N}(v)$, $\mathcal{L}^{(v)}$ is the minimal ideal in $\mathcal{L}$ such that $\mathcal{F}^0_{\gamma,-N} \in \mathcal{L}_k^{(v)}$ for all $\gamma \geqslant v$.

d) *Fundamental sequence of Lie algebras.*

Using the above equivalence of the categories of $p$-groups and Lie algebras we replace (0.1) by the exact sequence of Lie $\mathbb{F}_p$-algebras

$$0 \longrightarrow \bar{\mathcal{L}} \longrightarrow L \longrightarrow \mathbb{F}_p\tau_0 \longrightarrow 0\,, \tag{0.2}$$

where $\bar{\mathcal{L}} = \mathcal{L}/\mathcal{L}(p)$, $G(\mathcal{L}(p)) = \mathrm{Ker}\,\iota_{<p}$ and $G(L) = \Gamma_{<p}$. If $\tau_{<p}$ is a lift of $\tau_0$ to $L$ then the structure of (0.2) can be described via the differentiation $\mathrm{ad}\tau_{<p}$ on $\bar{\mathcal{L}}$.

e) *Replacing $\tau_0$ by $h \in \mathrm{Aut}\mathcal{K}$.*

When studying the structure of (0.2) we can approximate $\tau_0$ by a suitable $h \in \mathrm{Aut}\mathcal{K}$. This automorphism can be defined in terms of the expansion of $\zeta_1$ in powers of $\pi_0$. Then the formalism of nilpotent

Artin-Schreier theory allows us to specify a lift $\tau_{<p}$, to find the ideal $\mathcal{L}(p)$ and to introduce a recurrent procedure of obtaining the elements $\mathrm{ad}\tau_{<p}(D_{an}) := [D_{an}, \tau_{<p}] \in \bar{\mathcal{L}}_k$ and $\mathrm{ad}\tau_{<p}(D_0) := [D_0, \tau_{<p}] \in \bar{\mathcal{L}}$.

f) *Structure of $L$.*

Analyzing the above recurrent procedure modulo $C_2(\bar{\mathcal{L}})_k$ we will see that the knowledge of $\mathrm{ad}\tau_{<p}(D_{an})$ allows us to kill all generators $D_{an}$ of $\bar{\mathcal{L}}_k$ with $a > e^* := e_K p/(p-1)$. (Here $e_K$ is the ramification index of $K$ over $\mathbb{Q}_p$.) In other words, $L_k$ has a minimal system of generators $\{D_{an} \mid 1 \leqslant a < e^*, n \in \mathbb{Z}/N_0\} \cup \{D_0\} \cup \{\tau_{<p}\}$. On the other hand, $\mathrm{ad}\tau_{<p}(D_0) \in C_2(\bar{\mathcal{L}}) \subset C_2(L)$ and, therefore, gives us the Demushkin relation in $L$.

The following two steps will be done in the second part [8].

g) *Ramification ideals $L^{(v)}$ in $L$.*

For $v > e^*$, all ramification ideals $L^{(v)}$ are contained in $\bar{\mathcal{L}}$ and come from the appropriate ideals $\mathcal{L}^{(v')}$, where the upper indices $v$ and $v'$ are related by the Herbrand function $\varphi_{\widetilde{K}/K}$ of the field extension $\widetilde{K}/K$. As one of immediate applications we found for $2 \leqslant s < p$, the biggest upper ramification numbers $v[s]$ of the maximal $p$-extensions $K[s]$ of $K$ with the Galois groups of period $p$ and nilpotent class $\leqslant s$. We obtain the remaining ramification ideals $L^{(v)}$ with $v \leqslant e^*$ by specifying "good" lifts $\tau_{<p}$ (i.e. such that $\tau_{<p} \in L^{(e^*)}$) of $\tau_0$.

h) *Explicit formulas for* $\mathrm{ad}\tau_{<p}$ *with "good" $\tau_{<p}$.*

The formulas for $\mathrm{ad}\tau_{<p}(D_{an})$ and $\mathrm{ad}\tau_{<p}(D_0)$ are obtained modulo $C_3(L_k)$ as a second central step in the recurrent procedure from e), cf. Subsection 3.6 of this paper. In [8] we obtain a general formula for $\mathrm{ad}\tau_{<p}(D_0)$. This will give us an explicit form of the Demushkin relation in terms of the ramification generators $\mathcal{F}^0_{\gamma,-N}$ from c).

As a matter of fact, in both papers we work mostly with the automorphism $h$ and only in the very end prove that all results obtained in the context of $h$ also hold with $\tau_0$.

0.2. **Main results.** Introduce the weights $\mathrm{wt}(l)$ of elements $l \in \mathcal{L}_k$ by setting $\mathrm{wt}(D_{an}) = s \in \mathbb{N}$ if $(s-1)e^* \leqslant a < se^*$.

**Theorem 0.1.** a) $\mathcal{L}(p) = \{l \in \mathcal{L} \mid \mathrm{wt}(l) \geqslant p\}$;

b) *if* $\mathcal{L}(s) = \{l \in \mathcal{L} \mid \mathrm{wt}(l) \geqslant s\}$ *then* $C_s(L) = \mathcal{L}(s)/\mathcal{L}(p)$.

Suppose for all $a$, $V_{a0} \in \bar{\mathcal{L}}_k$ are such that $\mathrm{ad}\tau_{<p}(D_{a0}) = V_{a0}$. In particular, $V_{00} = \alpha_0 V_0$, where $V_0 = (\mathrm{ad}\tau_{<p})D_0 \in \bar{\mathcal{L}}$. The knowledge of these elements determines uniquely the differentiation $\mathrm{ad}\tau_{<p}$ (note that for all $n$, $\mathrm{ad}\tau_{<p}(D_{an}) = \sigma^n(V_{a0})$).

Suppose $E(X) = \exp(X + X^p/p + \cdots + X^{p^n}/p^n + \dots) \in \mathbb{Z}_p[[X]]$ is the Artin-Hasse exponential.

Let $\omega(t) \in k[[t]]$ be such that $E(\omega(\pi_0)) = \zeta_1 \bmod p$.

**Theorem 0.2.** *The elements $V_{a0}$ can be found from the following recurrent relation in $\bar{\mathcal{L}}_{\mathcal{K}}$*

$$\sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_{a0} =$$

$$-\sum_{k \geqslant 1} \frac{1}{k!}\, t^{-(a_1+\cdots+a_k)} \omega(t)^p [\ldots[a_1 D_{a_1 0}, D_{a_2 0}], \ldots, D_{a_k 0}]$$

$$-\sum_{k \geqslant 2} \frac{1}{k!} t^{-(a_1+\cdots+a_k)} [\ldots[V_{a_1}, D_{a_2 0}], \ldots, D_{a_k 0}]$$

$$-\sum_{k \geqslant 1} \frac{1}{k!}\, t^{-(a_1+\cdots+a_k)} [\ldots[\sigma c_1, D_{a_1 0}], \ldots, D_{a_k 0}],$$

*where in all last three sums the indices $a_1, \ldots, a_k$ run over the set $\mathbb{Z}^0(p) := \mathbb{Z}^+(p) \cup \{0\}$.*

In the above system of equations we are looking for the solutions of the form $\{c_1 \in \bar{\mathcal{L}}_{\mathcal{K}}, \{V_{a0} \in \bar{\mathcal{L}}_k \mid a \in \mathbb{Z}^0(p)\}\}$. These solutions correspond to different choices of the lift $\tau_{<p}$ of $\tau_0$, in particular, $c_1$ is a strict invariant of a lift $\tau_{<p}$. Actually, we have more: if $c_1 = \sum_{i \in \mathbb{Z}} c_1(i) t^i$ with all $c_1(i) \in \bar{\mathcal{L}}_k$, then $c_1(0)$ is a strict invariant of $\tau_{<p}$.

The content of this paper is arranged in a slightly different order compared to above principal steps a)-f). In Section 1 we briefly discuss auxiliary facts and constructions from the characteristic $p$ case. In Section 2 we study an analogue $\mathcal{G}_h$ of $\Gamma_{<p}$ which appears if we replace $\tau_0$ by a suitable $h \in \mathrm{Aut}\mathcal{K}$; we also describe the commutator subgroups of $\mathcal{G}_h$ and, in particular, find the ideal $\mathcal{L}(p)$. In Section 3 we develop the techniques allowing us to switch the languages of $p$-groups and Lie algebras. Finally, in Section 4 we prove that all our results obtained for the group $\mathcal{G}_h$ actually hold in the context of the group $\Gamma_{<p}$.

*Acknowledgements.* The author expresses deep gratitude to the referee: his advices allowed the author to avoid a considerable amount of inexactitudes and improve significantly the quality of the original exposition.

## 1. Preliminaries

1.1. **Covariant nilpotent Artin-Schreier theory.** Suppose $\mathcal{K}$ is a field of characteristic $p$, $\mathcal{K}_{sep}$ is a separable closure of $\mathcal{K}$ and $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$. We assume that the composition $g_1 g_2$ of $g_1, g_2 \in \mathcal{G}$ is such that for any $a \in \mathcal{K}_{sep}$, $g_1(g_2 a) = (g_1 g_2)a$.

In [1, 2, 3] the author developed a nilpotent analogue of the classical Artin-Schreier theory of cyclic field extensions of characteristic $p$.

The main results of this theory (which will be called the contravariant nilpotent Artin-Schreier theory) can be briefly explained as follows.

Let $\mathcal{G}^0$ be the group such that $\mathcal{G}^0 = \mathcal{G}$ as sets but for any $g_1, g_2 \in \mathcal{G}$ their composition in $\mathcal{G}^0$ equals $g_2 g_1$. In other words, we assume that $\mathcal{G}^0$ acts on $\mathcal{K}_{sep}$ via $(g_1 g_2)a = g_2(g_1(a))$.

Let $L$ be a Lie $\mathbb{F}_p$-algebra of nilpotent class $< p$. Then the absolute Frobenius $\sigma$ and $\mathcal{G}^0$ act on $L_{\mathcal{K}_{sep}}$ through the second factor. We have $L_{\mathcal{K}_{sep}}|_{\sigma=\mathrm{id}} = L$ and $(L_{\mathcal{K}_{sep}})^{\mathcal{G}^0} = L_{\mathcal{K}}$.

For any $e \in G(L_{\mathcal{K}})$, the set of $f \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f) = f \circ e$ is not empty. Define the group homomorphism $\pi_f^0(e) : \mathcal{G}^0 \to G(L)$ by setting for any $g \in \mathcal{G}^0$, $\pi_f^0(e) : g \mapsto g(f) \circ (-f)$.

**Remark.** Strictly speaking $g(f)$, where $g \in \mathcal{G}^0$, should be written in the form $(\mathrm{id}_L \otimes g)f$ but in most cases we use the first notation. On the other hand, we would prefer the second notation if, say, $g \in \mathrm{Aut}\mathcal{K}_{sep}$ and $g|_{\mathcal{K}} \neq \mathrm{id}_{\mathcal{K}}$. (Similarly, we have already agreed in the Introduction to use the notation $\sigma$ instead of $\mathrm{id}_L \otimes \sigma$.)

We have the following properties:

a) for any group homomorphism $\eta : \mathcal{G}^0 \to G(L)$ there are $e_\eta \in G(L_{\mathcal{K}})$ and $f_\eta \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f_\eta) = f_\eta \circ e_\eta$ and $\eta = \pi_{f_\eta}^0(e_\eta)$;

b) two homomorphisms $\pi_f^0(e)$ and $\pi_{f_1}^0(e_1)$ from $\mathcal{G}^0$ to $G(L)$ are conjugated via some element from $G(L)$ iff there is an $x \in G(L_{\mathcal{K}})$ such that $e_1 = (-x) \circ e \circ \sigma(x)$.

The covariant version of the above theory can be developed quite similarly. We just use the relations $\sigma(f) = e \circ f$ and $g \mapsto (-f) \circ g(f)$ to define the group homomorphism $\pi_f(e) : \mathcal{G} \longrightarrow G(L)$. Then we have the obvious analogs of above properties a) and b) with the opposite formula $e_1 = \sigma(x) \circ e \circ (-x)$ in the case b).

In this and next paper we use the covariant theory but need some results from [3] which were obtained in the contravariant setting. These results can be adjusted to the covariant theory just by replacing all involved group or Lie structures to the opposite ones, e.g. cf. Subsection 1.4 below.

1.2. **Lifts of analytic automorphisms.** Let $\mathrm{Aut}\,\mathcal{K}$ and $\mathrm{Aut}\,\mathcal{K}_{sep}$ be the groups of continuous automorphisms of $\mathcal{K}$ and $\mathcal{K}_{sep}$, respectively. For $h \in \mathrm{Aut}\,\mathcal{K}$, let $h_{sep} \in \mathrm{Aut}\,\mathcal{K}_{sep}$ be a lift of $h$, i.e. $h_{sep}|_{\mathcal{K}} = h$.

Suppose $L$ is a Lie $\mathbb{F}_p$-algebra of nilpotent class $< p$. Let $e \in G(L_{\mathcal{K}})$, choose $f \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f) = e \circ f$, set $\eta = \pi_f(e)$ and $\mathcal{K}_e = \mathcal{K}_{sep}^{\mathrm{Ker}\,\eta}$. Then $\mathcal{K}_e$ does not depend on a choice of $f$: if $f' \in G(L_{\mathcal{K}_{sep}})$ is such that $\sigma(f') = e \circ f'$ then $f' = f \circ l$ with $l \in G(L)$ and $\mathrm{Ker}\,\eta = \mathrm{Ker}\,\pi_{f'}(e)$.

**Proposition 1.1.** *Suppose $\eta : \mathcal{G} \longrightarrow G(L)$ is epimorphic. Then the following conditions are equivalent:*

a) $h_{sep}(\mathcal{K}_e) = \mathcal{K}_e$;

b) *there are* $c \in G(L_{\mathcal{K}})$ *and* $A \in \mathrm{Aut}L$ *such that* $(\mathrm{id}_L \otimes h_{sep})f = c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{sep}})f$.

*Proof.* Let $e_1 = (\mathrm{id}_L \otimes h)e$, $f_1 = (\mathrm{id}_L \otimes h_{sep})f$ and $\eta_1 = \pi_{f_1}(e_1)$. Then for any $g \in \mathcal{G}$, we have $\eta_1(g) = (-f_1) \circ g(f_1) =$

$$(\mathrm{id}_L \otimes h)((-f) \circ (h_{sep}^{-1}\, g\, h_{sep})f) = \eta(h_{sep}^{-1}\, g\, h_{sep}).$$

Therefore, $\eta_1$ is equal to the composition of the conjugation by $h_{sep}$ on $\mathcal{G}$ (we shall denote it by $\mathrm{Ad}\, h_{sep}$ below) and $\eta$. Then $h_{sep}(\mathcal{K}_e) = \mathcal{K}_e$ means that $\mathrm{Ker}\,\eta = \mathrm{Ker}\,\eta_1$. This implies the existence of an automorphism $A$ of the group $G(L)$ (which is automatically automorphism of the Lie algebra $L$) such that $\eta_1 = A\eta$.

Now let $f' = (A \otimes \mathrm{id}_{\mathcal{K}_{sep}})f$ and $e' = (A \otimes \mathrm{id}_{\mathcal{K}})e$. Then $\pi_{f'}(e')g = (A \otimes \mathrm{id}_{\mathcal{K}_{sep}})((-f) \circ g(f)) = (A\eta)g = \eta_1(g)$. This means that $f'$ and $f_1$ give the same morphisms $\mathcal{G} \to G(L)$ and there is $c \in G(L_{\mathcal{K}})$ such that $f_1 = c \circ f'$, that is a) implies b). Proceeding in the opposite direction we can deduce b) from a). □

**Remark.** From the proof of the above proposition it follows that a choice of the lift $h_{sep}$ uniquely determines its ingredients $c \in L_{\mathcal{K}}$ and $A \in \mathrm{Aut}_{Lie}L$. Indeed, $A$ appears as $\mathrm{Ad}(h_{sep}|_{\mathcal{K}_e})$ (with respect to the identification $\mathcal{G}/\mathrm{Ker}\,\eta = G(L)$ induced by $\eta$) and $c$ is recovered then as $(\mathrm{id}_L \otimes h_{sep})f \circ (A \otimes \mathrm{id}_{\mathcal{K}_{sep}})(-f)$. This shows that the couple $(c, A)$ depends only on the restriction $h_{sep}|_{\mathcal{K}_e}$ and we can consider the map $h_{sep}|_{\mathcal{K}_e} \mapsto (c, A)$ from the set of all lifts of $h$ to $\mathcal{K}_e$ to the set of appropriate couples $(c, A)$. But the knowledge of $(c, A)$ allows us to recover uniquely the element $(\mathrm{id}_{\mathcal{L}} \otimes h_{sep})f$ and the Galois group $\mathrm{Gal}(\mathcal{K}_e/\mathcal{K})$ acts strictly on the set of all such elements. Therefore, any couple $(c, A)$ appears from no more than one lift of $h$ to $\mathcal{K}_e$, that is the map $h_{sep}|_{\mathcal{K}_e} \mapsto (c, A)$ is injective. We will study this map in more details below, cf. Proposition 2.3.

1.3. **The identification** $\eta_0$**.** Let $\mathcal{K} = k((t))$ be a complete discrete valuation field of Laurent formal power series in variable $t$ with coefficients in $k \simeq \mathbb{F}_{p^{N_0}}$, $N_0 \in \mathbb{N}$. Choose $\alpha_0 \in k$ such that $\mathrm{Tr}_{k/\mathbb{F}_p}\alpha_0 = 1$.

Denote by $\widetilde{\mathcal{L}}_k$ a free pro-finite Lie algebra over $k$ with the set of free generators $\{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{D_0\}$. As earlier, denote by the same symbol $\sigma$, the $\sigma$-linear automorphism of $\widetilde{\mathcal{L}}_k$ such that $\sigma : D_0 \mapsto D_0$ and for all $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z}/N_0$, $\sigma : D_{an} \mapsto D_{a,n+1}$. Then $\widetilde{\mathcal{L}}^0 := \widetilde{\mathcal{L}}_k|_{\sigma=\mathrm{id}}$ is a free pro-finite Lie $\mathbb{F}_p$-algebra and $\widetilde{\mathcal{L}}_k = \widetilde{\mathcal{L}}^0_k$.

Let $\mathcal{L} = \widetilde{\mathcal{L}}^0/C_p(\widetilde{\mathcal{L}}^0)$.

For any $n \in \mathbb{Z}/N_0$, set $D_{0n} = \sigma^n(\alpha_0)D_0$.

Let $e = \sum_{a \in \mathbb{Z}^0(p)} t^{-a} D_{a0} \in G(\mathcal{L}_{\mathcal{K}})$ and fix a choice of $f \in G(\mathcal{L}_{\mathcal{K}_{sep}})$ such that $\sigma(f) = e \circ f$. Then the morphism $\eta = \pi_f(e)$ induces the isomorphism of topological groups $\eta_0 : \mathcal{G}_{<p} := \mathcal{G}/\mathcal{G}^p C_p(\mathcal{G}) \xrightarrow{\sim} G(\mathcal{L})$.

In the remaining part of the paper we use (without additional notice) the above introduced notation $e$, $f$, $\eta$ and $\eta_0$. The appropriate field $\mathcal{K}_e$ coincides with $\mathcal{K}_{sep}^{\mathcal{G}^p C_p(\mathcal{G})}$ and will be denoted by $\mathcal{K}_{<p}$.

Note that $f \in G(\mathcal{L}_{\mathcal{K}_{<p}})$. In particular, if $h_1, h_2 \in \operatorname{Aut}\mathcal{K}_{sep}$ are such that $h_1|_{\mathcal{K}} = h_2|_{\mathcal{K}}$ and $(\mathrm{id}_{\mathcal{L}} \otimes h_1)f = (\mathrm{id}_{\mathcal{L}} \otimes h_2)f$ then $h_1|_{\mathcal{K}_{<p}} = h_2|_{\mathcal{K}_{<p}}$, cf. Remark at the end of Subsection 1.2. Therefore, the appropriate choice of the ingredients $c \in \mathcal{L}_{\mathcal{K}}$ and $A \in \operatorname{Aut}\mathcal{L}$ from Proposition 1.1 can be used to describe efficiently the lifts of automorphisms $h$ of $\mathcal{K}$ to automorphisms $h_{<p}$ of $\mathcal{K}_{<p}$.

We also use in Subsection 2.2 and [8], Subsection 2.5, the following interpretation of this property:

– *if* $\mathcal{L}_1 \subset \mathcal{L}$ *is ideal and* $\mathcal{K}_{<p}^{G(\mathcal{L}_1)} = \mathcal{K}_1$ *then* $f \bmod \mathcal{L}_{1\mathcal{K}_{<p}} \in (\mathcal{L}/\mathcal{L}_1)_{\mathcal{K}_1}$, *or equivalently,* $f \in \mathcal{L}_{\mathcal{K}_1} + \mathcal{L}_{1\mathcal{K}_{<p}}$.

Note that $\eta : \mathcal{G} \longrightarrow G(\mathcal{L})$ induces (use $f \bmod \mathcal{L}_{1\mathcal{K}_{<p}}$) the identification $\mathrm{Gal}(\mathcal{K}_1/\mathcal{K}) \simeq G(\mathcal{L}/\mathcal{L}_1)$.

If $h \in \operatorname{Aut}\mathcal{K}$ then its lifts to $\operatorname{Aut}\mathcal{K}_{<p}$ will be denoted usually by $h_{<p}$. As we have already pointed out, $G(\mathcal{L})$ acts transitively on the set of all lifts $h_{<p}$ of a given $h$: for any $l \in G(\mathcal{L})$, $h_{<p} \mapsto h_{<p} * l = h_{<p}\,\eta_0^{-1}(l)$.

1.4. **The ramification subgroups in $\mathcal{G}_{<p}$.** For $v \geqslant 0$, let $\mathcal{G}_{<p}^{(v)}$ be the image of the ramification subgroup $\mathcal{G}^{(v)}$ of $\mathcal{G}$ in $\mathcal{G}_{<p}$. This subgroup corresponds to some ideal $\mathcal{L}^{(v)}$ of the Lie algebra $\mathcal{L}$ with respect to the identification $\eta_0$.

When working with the above standard generators of $\mathcal{L}_k$ we very often denote them by $D_{an}$, where $n \in \mathbb{Z}$, by having in mind that they depend only on the residue of $n$ modulo $N_0$, i.e. $D_{an} := D_{a,n \bmod N_0}$.

For $\gamma \geqslant 0$ and $N \in \mathbb{N}$, introduce $\mathcal{F}^0_{\gamma,-N} \in \mathcal{L}_k$ such that

$$\mathcal{F}^0_{\gamma,-N} = \sum_{\substack{1 \leqslant s < p \\ a_i, n_i}} a_1 \eta(n_1, \dots, n_s)[\dots[D_{a_1 n_1}, D_{a_2 n_2}], \dots, D_{a_s n_s}]$$

Here:

— $a_1 p^{n_1} + a_2 p^{n_2} + \dots + a_s p^{n_s} = \gamma$;

— if $0 = n_1 = \dots = n_{s_1} > \dots > n_{s_{r-1}+1} = \dots = n_{s_r} \geqslant -N$ then $\eta(n_1, \dots, n_s) = (s_1! \dots (s_r - s_{r-1})!)^{-1}$; otherwise, $\eta(n_1, \dots, n_s) = 0$.

**Theorem 1.2.** *For any $v \geqslant 0$, there is $\widetilde{N}(v)$ such that if $N \geqslant \widetilde{N}(v)$ is fixed then the ideal $\mathcal{L}^{(v)}$ is the minimal ideal in $\mathcal{L}$ such that its extension of scalars $\mathcal{L}_k^{(v)}$ contains all $\mathcal{F}^0_{\gamma,-N}$ with $\gamma \geqslant v$.*

The appropriate theorem in the contravariant setting was obtained in [1] (or in a more general form in the context of groups of period $p^M$ in [3]) and uses the elements $\mathcal{F}_{\gamma,-N}$ given by the same formula but with the

factor $(-1)^{s-1}$. Indeed, when switching to the covariant setting all commutators of the form $[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_sn_s}]$ should be replaced by $[D_{a_sn_s}, \dots, [D_{a_2n_2}, D_{a_1n_1}]\dots] = (-1)^{s-1}[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_sn_s}]$.

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

2.1. **The automorphism $h$.** Let $c_0 \in p\mathbb{N}$. Denote by $h$ a continuous automorphism of $\mathcal{K}$ such that $h|_k = \mathrm{id}$ and

$$h(t) = t\left(1 + \sum_{i\geqslant 0} \alpha_i(h) t^{c_0+pi}\right),$$

where all $\alpha_i(h) \in k$ and $\alpha_0(h) \neq 0$. This automorphism will be fixed in the remaining part of the paper.

As earlier, $E(X) = \exp\left(\sum_{i\geqslant 0} X^{p^i}/p^i\right) \in \mathbb{Z}_p[[X]]$.

**Proposition 2.1.**

a) *There is $\omega_h \in t^{c_0/p}O_{\mathcal{K}}^*$ such that $h(t) = tE(\omega_h^p)$;*

b) *For any $n \geqslant 0$, $h^n(t) \equiv tE(n\omega_h^p) \bmod t^{1+pc_0}$.*

*Proof.* For part a), $\omega_h$ appears as a unique element from $tk[[t]]$ such that $E(\omega_h) = 1 + \sum_{j\geqslant 0} \sigma^{-1}(\alpha_j(h)) t^{c_0/p+j}$. (Use that $x \mapsto E(x) - 1$ is bijective on $tk[[t]]$.) For part b), note that $h(t) \equiv t \bmod t^{c_0}$ implies that $h(t^{c_0+pi}) \equiv t^{c_0+pi} \bmod t^{pc_0}$ and, therefore, $h(\omega_h^p) \equiv \omega_h^p \bmod t^{pc_0}$. Now apply induction on $n$. If our proposition is proved for $n \geqslant 1$ then

$$h^{n+1}(t) \equiv h(t)h(E(n\omega_h^p)) \equiv tE(\omega_h^p)E(n\omega_h^p) \equiv tE((n+1)\omega_h^p) \bmod t^{pc_0+1}$$

(use that $E(X+Y) \equiv E(X)E(Y) \bmod \deg p$). □

**Remark.** In all applications below the knowledge of the automorphism $h$ will be essential only modulo $t^{1+pc_0}$ and, therefore, in the above proposition we can use instead of $E(X)$ the truncated exponential $\widetilde{\exp}(X) = 1 + X + \dots + X^{p-1}/(p-1)!$.

2.2. **Operators $\mathcal{R}$ and $\mathcal{S}$.** Suppose $\mathfrak{M}$ is a profinite $\mathbb{F}_p$-module. Define the continuous $\mathbb{F}_p$-linear operators $\mathcal{R}, \mathcal{S} : \mathfrak{M}_{\mathcal{K}} \longrightarrow \mathfrak{M}_{\mathcal{K}}$ as follows.

Suppose $\alpha \in \mathfrak{M}_k$.

If $n > 0$ then 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 $\mathcal{R}(\alpha) = \alpha_0 \mathrm{Tr}_{k/\mathbb{F}_p}\alpha$, $\mathcal{S}(\alpha) = \sum_{0\leqslant j<i<N_0} (\sigma^j\alpha_0)\sigma^i\alpha$.

If $n = -n_1p^m < 0$ with $\gcd(n_1, p) = 1$ then set $\mathcal{R}(t^n\alpha) = t^{-n_1}\sigma^{-m}\alpha$ and $\mathcal{S}(t^n\alpha) = \sum_{1\leqslant i\leqslant m} \sigma^{-i}(t^n\alpha)$.

The proof of the following lemma is straightforward.

**Lemma 2.2.** *For any $b \in \mathfrak{M}_{\mathcal{K}}$,*

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

b) *if $b = b_1 + \sigma b_2 - b_2$, where $b_1 \in \sum_{a\in\mathbb{Z}^+(p)} t^{-a}\mathfrak{M}_k + \alpha_0\mathfrak{M}$ and $b_2 \in \mathfrak{M}_{\mathcal{K}}$ then $b_1 = \mathcal{R}(b)$ and $b_2 - \mathcal{S}(b) \in \mathfrak{M}$.*

**Remark.** A typical situation where we refer to the above lemma appears as follows: suppose $\mathfrak{N} \subset \mathfrak{M}$ is an $\mathbb{F}_p$-submodule and

$$b = \sum_{a \in \mathbb{Z}^+(p)} t^{-a} b_a + \alpha_0 b_0 + \sigma c - c\,,$$

with all $b_a \in \mathfrak{M}_k$, $b_0 \in \mathfrak{M}$ and $c \in \mathfrak{M}_{\mathcal{K}}$; if $b \in \mathfrak{N}_{\mathcal{K}}$ then all $b_a \in \mathfrak{N}_k$, $b_0 \in \mathfrak{N}$ and $c \in \mathfrak{M} + \mathfrak{N}_{\mathcal{K}}$.

2.3. **Specification of $h_{<p}$.** We are going to specify a lift $h^0_{<p}$ of $h$ to $\mathcal{K}_{<p}$ by using formalism of nilpotent Artin-Schreier theory. Recall that for any lift $h_{<p}$ of $h$, we have a unique $c \in \mathcal{L}_{\mathcal{K}}$ and $A = \mathrm{Ad}\, h_{<p} \in \mathrm{Aut}\, \mathcal{L}$ such that $(\mathrm{id}_{\mathcal{L}} \otimes h_{<p})f = c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$. The map $h_{<p} \mapsto (c, A)$ is injective, cf. Subsection 1.2. The following proposition describes the image of this map.

**Proposition 2.3.** *The correspondence $\Pi : h_{<p} \mapsto (c, A)$ induces a bijection of the set of all lifts $h_{<p}$ of $h$ and the set of pairs $(c, A) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\, \mathcal{L}$ such that*

$$(\mathrm{id}_{\mathcal{L}} \otimes h)e \circ c = \sigma c \circ (A \otimes \mathrm{id}_{\mathcal{K}})e\,. \tag{2.1}$$

*Proof.* If $\Pi(h_{<p}) = (c, A)$ then

$$(\mathrm{id}_{\mathcal{L}} \otimes h)e \circ (\mathrm{id}_{\mathcal{L}} \otimes h_{<p})f = (\mathrm{id}_{\mathcal{L}} \otimes h_{<p})(e \circ f) = (\mathrm{id}_{\mathcal{L}} \otimes h_{<p})\sigma f =$$
$$\sigma c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})\sigma f = \sigma c \circ (A \otimes \mathrm{id}_{\mathcal{K}})e \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$$
$$= \sigma c \circ (A \otimes \mathrm{id}_{\mathcal{K}})e \circ (-c) \circ (\mathrm{id}_{\mathcal{L}} \otimes h_{<p})f\,.$$

This proves that $(c, A)$ satisfies identity (2.1).

Let $l' \in \mathcal{L}$. Then $\eta_0^{-1}(l') \in \mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K})$ and $h_{<p}\,\eta_0^{-1}(l')$ is again a lift of $h$ to $\mathcal{K}_{<p}$. Therefore, we have a transitive action $h_{<p} \mapsto h_{<p} * l' := h_{<p}\eta_0^{-1}(l')$ of $G(\mathcal{L})$ on the set of all lifts $h_{<p}$.

At the same time, if $(c, A)$ satisfies (2.1) then the new couple $(c, A) * l' := (c \circ (l' \otimes 1), (\mathrm{Ad}\, l')A)$ is again a solution of (2.1). Indeed,

$$(\mathrm{id}_{\mathcal{L}} \otimes h)e \circ c \circ (l' \otimes 1) = (\sigma c) \circ (A \otimes \mathrm{id}_{\mathcal{K}})e \circ (l' \otimes 1)$$
$$= \sigma(c \circ (l' \otimes 1)) \circ (-l' \otimes 1) \circ (A \otimes \mathrm{id}_{\mathcal{K}})e \circ (l' \otimes 1)\,,$$

and $(-l' \otimes 1) \circ (A \otimes \mathrm{id}_{\mathcal{K}}) \circ (l' \otimes 1)$ acts on $\mathcal{L}_{\mathcal{K}}$ as $(\mathrm{Ad}\, l')A \otimes \mathrm{id}_{\mathcal{K}}$, i.e. $\mathrm{Ad}(l' \otimes 1) : \mathcal{L}_{\mathcal{K}} \longrightarrow \mathcal{L}_{\mathcal{K}}$ is $\mathcal{K}$-linear. (Indeed, one of most known properties of Campbell-Hausdorff formula, cf. [9], Ch.II, Section 6.5, gives that

$$(-l' \otimes 1) \circ l \circ (l' \otimes 1) = \sum_{0 \leqslant i < p} [\ldots [l, \underbrace{l' \otimes 1], \ldots, l' \otimes 1}_{i \text{ times}}]/i!$$

depends linearly on $l \in \mathcal{L}_{\mathcal{K}}$. )

This defines the action $(c, A) \mapsto (c, A) * l'$ of $G(\mathcal{L})$ on all solutions $(c, A)$ of (2.1). Verify that the map $\Pi$ is compatible with above defined $G(\mathcal{L})$-actions. Indeed, if $\Pi(h_{<p}) = (c, A)$ then $h_{<p} * l'$ sends $f$ to

$$h_{<p}(f \circ (l' \otimes 1)) = c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f \circ (l' \otimes 1) =$$

$$(c \circ (l' \otimes 1)) \circ (-l' \otimes 1) \circ (A \otimes \mathrm{id}_{K_{<p}}) f \circ (l' \otimes 1)$$

and therefore, $\Pi(h_{<p} * l') = (c, A) * l'$. So, our proposition will be proved if we show that $G(\mathcal{L})$ acts transitively on the set of all solutions $(c, A)$ of (2.1).

Suppose $(c, A)$ and $(c', A')$ are solutions of (2.1). Then the existence of $l' \in G(\mathcal{L})$ such that $(c', A') = (c, A) * l'$ will be implied by the following lemma.

**Lemma 2.4.** *For any $1 \leqslant s \leqslant p$, there is $l'_s \in G(\mathcal{L})$ such that if $(c'_s, A'_s) = (c, A) * l'_s$ then $c_s \equiv c' \bmod C_s(\mathcal{L}_\mathcal{K})$ and $A_s \equiv A' \bmod C_s(\mathcal{L})$.*

*Proof of lemma.* Use induction on $s$.

If $s = 1$ there is nothing to prove.

Suppose lemma is proved for some $1 \leqslant s < p$.

Let $c' = c'_s + \delta$ and $A' = A'_s + \mathcal{A}$, where $\delta \in C_s(\mathcal{L}_\mathcal{K})$ and $\mathcal{A} \in \mathrm{Hom}_{\mathbb{F}_p - \mathrm{mod}}(\mathcal{L}, C_s(\mathcal{L}))$. Then we have modulo $C_{s+1}(\mathcal{L}_\mathcal{K})$:

$$(\mathrm{id}_\mathcal{L} \otimes h) e \circ c' \equiv (\mathrm{id}_\mathcal{L} \otimes h) e \circ c'_s + \delta\,,$$

$$(\sigma c') \circ (A' \otimes \mathrm{id}_\mathcal{K}) e \equiv (\sigma c'_s) \circ (A'_s \otimes \mathrm{id}_\mathcal{K}) e + \sigma(\delta) + (\mathcal{A} \otimes \mathrm{id}_\mathcal{K}) e\,.$$

Because $(c'_s, A'_s)$ and $(c', A')$ are solutions of (2.1) we obtain

$$\sigma\delta - \delta + \sum_{a \in \mathbb{Z}^+(p)} t^{-a} \mathcal{A}_k(D_{a0}) + \alpha_0 \mathcal{A}(D_0) \in C_{s+1}(\mathcal{L}_\mathcal{K})\,,$$

where $\mathcal{A}_k = \mathcal{A} \otimes k \in \mathrm{Hom}_{k-\mathrm{mod}}(\mathcal{L}_k, C_s(\mathcal{L}_k))$. Now Lemma 2.2b) (cf. also remark b) after that lemma) implies that $\delta \equiv \delta_0 \bmod C_{s+1}(\mathcal{L}_\mathcal{K})$, where $\delta_0 \in C_s(\mathcal{L}) \otimes 1$, all $\mathcal{A}_k(D_{a0}) \in C_{s+1}(\mathcal{L}_k)$ and $\mathcal{A}(D_0) \in C_{s+1}(\mathcal{L})$. Therefore, modulo $C_{s+1}(\mathcal{L}_k)$ the automorphisms $A'$ and $A'_s$ coincide on generators of $\mathcal{L}_k$ (use that $\mathcal{A}_k(D_{an}) = \sigma^n \mathcal{A}_k(D_{a0})$ for all $n \in \mathbb{Z}/N_0$) and $A' \equiv A'_s \bmod C_{s+1}(\mathcal{L})$.

So, for $(c, A) * (l'_s \circ \delta) = (c'_s, A'_s) * \delta = (c'_{s+1}, A'_{s+1})$, we have that

$$c'_{s+1} = c'_s \circ \delta \equiv c'_s + \delta \equiv c' \bmod C_{s+1}(\mathcal{L}_\mathcal{K})$$

and

$$A'_{s+1} = (\mathrm{Ad}\,\delta) A'_s \equiv (\mathrm{Ad}\,\delta) A' \equiv A' \bmod C_{s+1}(\mathcal{L})\,.$$

The lemma and Proposition 2.3 are completely proved. □

□

**Remark.** Suppose $(c_1, A_1)$ and $(c_2, A_2)$ satisfy the identity (2.1) and $c_1 \equiv c_2 \bmod C_s(\mathcal{L}_\mathcal{K})$. Then $(A_1 \otimes \mathrm{id}_\mathcal{K}) e \equiv (A_2 \otimes \mathrm{id}_\mathcal{K}) e \bmod C_s(\mathcal{L}_\mathcal{K})$ and this implies that $A_1 \equiv A_2 \bmod C_s(\mathcal{L})$. In particular, if $\Pi(h_{<p}) = (c, A)$ then the restriction $h_{<s}$ of $h_{<p}$ to $\mathcal{K}_{<p}^{C_s(\mathcal{L})}$ is uniquely determined by the residue $c \bmod C_s(\mathcal{L}_\mathcal{K})$. Now from the proof of the above proposition it follows that all lifts of a given $h_{<s}$ to automorphisms $h_{<s+1}$ of $\mathcal{K}_{<p}^{C_{s+1}(\mathcal{L})}$ are uniquely determined by the residues $(c+\delta, A) \bmod C_{s+1}(\mathcal{L}_\mathcal{K})$, where $\delta \in C_s(\mathcal{L})$.

Using the above proposition and operators $\mathcal{R}$ and $\mathcal{S}$ from Subsection 2.2 we can specify a unique choice $h^0_{<p}$ in the set of all lifts of $h$ by specifying a unique solution $(c^0, A^0)$ of (2.1) as follows.

Suppose $1 \leqslant s < p$ and we have chosen $(c_s, A_s) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\mathcal{L}$ such that the identity (2.1) holds modulo $C_s(\mathcal{L}_{\mathcal{K}})$. If $s = 1$ we just choose $c_1 = 0$ and $A_1 = \mathrm{id}_{\mathcal{L}}$. Then we can find the solution $(c_{s+1}, A_{s+1}) \in \mathcal{L}_{\mathcal{K}} \times \mathrm{Aut}\,\mathcal{L}$ of (2.1) modulo $C_{s+1}(\mathcal{L}_{\mathcal{K}})$ by setting $c_{s+1} = c_s + X_s$ and $A_{s+1} = A_s + B_s$ where $X_s \in C_s(\mathcal{L}_{\mathcal{K}})$ and $B_s \in \mathrm{Hom}_{\mathbb{F}_p\text{-mod}}(\mathcal{L}, C_s(\mathcal{L}))$ must satisfy the relation

$$\sigma X_s - X_s + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} B_s(D_{a0}) \equiv \tag{2.2}$$

$$(\mathrm{id}_{\mathcal{L}} \otimes h)e \circ c_s - \sigma c_s \circ (A_s \otimes \mathrm{id}_{\mathcal{K}})e \bmod C_{s+1}(\mathcal{L}_{\mathcal{K}})\,.$$

By Lemma 2.2b) the recurrence relation (2.2) uniquely determines the elements $B_s(D_{a0}) \bmod C_{s+1}(\mathcal{L}_k)$ but the element $X_s$ is determined only up to elements of $C_s(\mathcal{L}) \bmod C_{s+1}(\mathcal{L})$. (This will affect the right-hand side of (2.2) at the next $(s+1)$-th step and so on.) Note that the knowledge of the elements $B_s(D_{a0}) \bmod C_{s+1}(\mathcal{L}_k)$ determines uniquely the automorphism $A_{s+1}$ modulo $C_{s+1}(\mathcal{L})$ because for all $n \in \mathbb{Z}/N_0$, $A_{s+1}(D_{an}) = \sigma^n A_{s+1}(D_{a0})$. By Proposition 2.3 all solutions $X_s$ correspond to different extensions of a given automorphism of $\mathcal{K}^{C_s(\mathcal{L})}_{<p}$ to an automorphism of $\mathcal{K}^{C_{s+1}(\mathcal{L})}_{<p}$ (cf. also the remark after the proof of that proposition). In particular, we can uniquely specify the lift $h^0_{<p}$ by specifying $(\mathrm{id}_{\mathcal{L}} \otimes h^0_{<p})f$ if we take at each $s$-th step the solutions of (2.2) in the form $\sum_{a \in \mathbb{Z}^0(p)} t^{-a} B_s(D_{a0}) = \mathcal{R}(\mathcal{B}_s)$ and $X_s = \mathcal{S}(\mathcal{B}_s)$, where $\mathcal{B}_s$ is the RHS in (2.2). As a result, the pair $(c^0, A^0) := (c_p, A_p)$ satisfies the identity (2.1) and defines the lift $h^0_{<p}$.

**Remark.** It is not easy to control the lifts $h_{<p}$ because condition (2.2) contains highly non-trivial Campbell-Hausdorff operation $\circ$. In Section 3 we resolve this problem by introducing the procedure of linearization.

2.4. **The group $\widetilde{\mathcal{G}}_h$.** Denote by $\widetilde{\mathcal{G}}_h$ the group of all lifts $\tilde{h}_{<p} \in \mathrm{Aut}\,\mathcal{K}_{<p}$ of the elements $\tilde{h}$ of the closed subgroup in $\mathrm{Aut}\,\mathcal{K}$ generated by $h$.

Use the identification $\eta_0$ from Subsection 1.3 to obtain a natural short exact sequence of profinite $p$-groups

$$1 \longrightarrow G(\mathcal{L}) \longrightarrow \widetilde{\mathcal{G}}_h \longrightarrow \langle h \rangle \longrightarrow 1 \tag{2.3}$$

For any $s \geqslant 2$, $C_s(\widetilde{\mathcal{G}}_h)$ is a subgroup in $G(\mathcal{L})$ and, therefore, $\mathcal{L}_h(s) := C_s(\widetilde{\mathcal{G}}_h)$ is a Lie subalgebra of $\mathcal{L}$. Set $\mathcal{L}_h(1) = \mathcal{L}$. Note that for any $s_1, s_2 \geqslant 1$, we have $[\mathcal{L}_h(s_1), \mathcal{L}_h(s_2)] \subset \mathcal{L}_h(s_1 + s_2)$.

Recall that the weight filtration $\mathcal{L}(s)$, $s \in \mathbb{N}$, in $\mathcal{L}$ was defined by setting $\mathrm{wt}(D_{an}) = s$ if $(s-1)c_0 \leqslant a < sc_0$. With this notation $\mathcal{L}(s)_k$ is generated over $k$ by all $[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_rn_r}]$ such that $\sum_i \mathrm{wt}(D_{a_in_i}) \geqslant s$. For any $s_1, s_2 \geqslant 1$, we also have that $[\mathcal{L}(s_1), \mathcal{L}(s_2)] \subset \mathcal{L}(s_1+s_2)$.

**Theorem 2.5.** *For all $s \in \mathbb{N}$, $\mathcal{L}_h(s) = \mathcal{L}(s)$.*

*Proof.* Let $h^0_{<p}$ be the lift constructed at the end of Subsection 2.3. Then $h^0_{<p} \in \widetilde{\mathcal{G}}_h$ is a preimage of $h$ in short exact sequence (2.3).

Let $\mathcal{L}^{lin} = (\sum_{a,n} kD_{an})|_{\sigma=\mathrm{id}}$ be "the subspace of linear terms" of $\mathcal{L}$. We have the following properties:

- $\mathcal{L}(s+1) = \mathcal{L}^{lin} \cap \mathcal{L}(s+1) + \mathcal{L}(s+1) \cap C_2(\mathcal{L})$;
- $\mathcal{L}(s+1) \cap C_2(\mathcal{L}) = \sum_{s_1+s_2=s+1} [\mathcal{L}(s_1), \mathcal{L}(s_2)]$;
- $\mathcal{L}_h(s+1)$ is the ideal in $\mathcal{L}$ generated by $[\mathcal{L}_h(s), \mathcal{L}]$ and the elements of the form $(\mathrm{Ad}\, h^0_{<p})l \circ (-l)$, where $l \in \mathcal{L}_h(s)$.

Let $(\mathrm{Ad}\, h^0_{<p})D_0 = \widetilde{D}_0$ and for all $a \in \mathbb{Z}^+(p)$, $(\mathrm{Ad}\, h^0_{<p})D_{a0} = \widetilde{D}_{a0}$.

**Lemma 2.6.** *We have:*

a) $\widetilde{D}_0 \equiv D_0 \bmod (\mathcal{L}(3) + \mathcal{L}(2) \cap C_2(\mathcal{L}))$;

b) *if $a \in \mathbb{Z}^+(p)$ and $\mathrm{wt}(D_{an}) = s$ then*

$$\widetilde{D}_{a0} \equiv D_{a0} - \sum_{i \geqslant 0} \alpha_i(h) a D_{a+c_0+pi,0} \bmod (\mathcal{L}(s+2)_k + \mathcal{L}(s+1)_k \cap C_2(\mathcal{L}_k)),$$

*where $\alpha_i(h) \in k$ are such that $h(t) = t(1 + \sum_{i \geqslant 0} \alpha_i(h) t^{c_0+pi})$.*

We prove this Lemma below after finishing the proof of Theorem 2.5. Clearly, Lemma 2.6 has the following corollaries:

(c1) *if $l \in \mathcal{L}(s)$ then $(\mathrm{Ad}\, h^0_{<p})l \circ (-l) \in \mathcal{L}(s+1)$;*

(c2) *if $l \in \mathcal{L}^{lin} \cap \mathcal{L}(s+1)$ then there is an $l' \in \mathcal{L}^{lin} \cap \mathcal{L}(s)$ such that* $\mathrm{Ad}\, h^0_{<p}(l') \circ (-l') \equiv l \bmod \mathcal{L}(s+1) \cap C_2(\mathcal{L})$ (use that $\alpha_0(h) \neq 0$).

Prove theorem by induction on $s \geqslant 1$.

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

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

Then $[\mathcal{L}_h(s_0), \mathcal{L}] = [\mathcal{L}(s_0), \mathcal{L}(1)] \subset \mathcal{L}(s_0+1)$ and applying (c1) 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 (c2) we obtain that $\mathcal{L}^{lin} \cap \mathcal{L}(s_0+1) \subset \mathcal{L}_h(s_0+1)$. So, $\mathcal{L}(s_0+1) \subset \mathcal{L}_h(s_0+1)$ and Theorem 2.5 is completely proved. $\square$

*Proof of Lemma 2.6.* Let

$$\mathcal{N}=\sum_{s\geqslant 1}t^{-c_0s}\mathcal{L}(s)_{\mathrm{m}},$$

where m is the maximal ideal of the valuation ring $O_{\mathcal{K}}$ of $\mathcal{K}$. Clearly, $\mathcal{N}$ has the structure of Lie algebra over $\mathbb{F}_p$.

Let

$$\tilde{e}:=(\mathrm{Ad}\,h^0_{<p}\otimes\mathrm{id}_{\mathcal{K}})e=\sum_{a\in\mathbb{Z}^+(p)}t^{-a}\widetilde{D}_{a0}+\alpha_0\widetilde{D}_0\,.$$

Then recovering $\tilde{e}$ from the following relation

$$(\mathrm{id}_{\mathcal{L}}\otimes h)e\circ c^0=(\sigma c^0)\circ\tilde{e}\,, \tag{2.4}$$

where $c^0\in G(\mathcal{L}_{\mathcal{K}})$, is a part of the procedure of specifying $h^0_{<p}$ described at the end of Subsection 2.3, i.e. $\tilde{e}=(A^0\otimes\mathrm{id}_{\mathcal{K}})e$.

Now note that $e\in\mathcal{N}$ and the operators $\mathcal{R}$ and $\mathcal{S}$ map $\mathcal{N}$ to itself. Therefore, when following the procedure of specifying $h^0_{<p}$ at each step we obtain that $\mathcal{B}_s,\mathcal{R}(\mathcal{B}_s),\mathcal{S}(\mathcal{B}_s)\in\mathcal{N}$ and, therefore, $\tilde{e},c^0,\sigma c^0\in\mathcal{N}$.

For any $i\geqslant 0$, introduce the ideals $\mathcal{N}(i):=t^{c_0i}\mathcal{N}$ of $\mathcal{N}$. Note that for all $i\geqslant 0$, the operators $\mathcal{R}$ and $\mathcal{S}$ map $\mathcal{N}(i)$ to itself.

Consider the following properties:

a) $(\mathrm{id}_{\mathcal{L}}\otimes h)e=e+e_1\bmod\mathcal{N}(2)$, where $e_1=e_1^++e_1^-\in\mathcal{N}(1)$ with

$$e_1^-=-\sum_{\substack{i\geqslant 0\\ a\in\mathbb{Z}^+(p)}}t^{-a}a\alpha_i(h)D_{a+c_0+pi,0},\ \ e_1^+=-\sum_{\substack{i\geqslant 0\\ 0<a<c_0+pi}}a\alpha_i(h)t^{-a+c_0+pi}D_{a0}$$

(note that $e_1^+\in\mathcal{L}_{\mathrm{m}}$ and, therefore, $\mathcal{R}(e_1^+)=0$);

b) the congruence $(\mathrm{id}_{\mathcal{L}}\otimes h)e\equiv e\bmod\mathcal{N}(1)$ implies that $\tilde{e}\equiv e\bmod\mathcal{N}(1)$ and $c^0,\sigma c^0\in\mathcal{N}(1)$: indeed, in the procedure of specifying $h^0_{<p}$ we have for all $s$, that $c_s,\sigma c_s\in\mathcal{N}(1)$ and $(A_s\otimes\mathrm{id}_{\mathcal{K}})e\equiv e\bmod\mathcal{N}(1)$;

c) $\tilde{e}=(-\sigma c^0)\circ(\mathrm{id}_{\mathcal{L}}\otimes h)e\circ c^0\equiv(c^0-\sigma c^0)+e+e_1\bmod\mathcal{N}(2)+t^{c_0}\widetilde{\mathcal{N}}^{(2)}$, where $\widetilde{\mathcal{N}}^{(2)}:=\sum_{s\geqslant 2}t^{-sc_0}(\mathcal{L}(s)\cap C_2(\mathcal{L}))_{\mathrm{m}}$ (use that $[\mathcal{N}(1),\mathcal{N}(1)]\subset\mathcal{N}(2)$ and $[\mathcal{N}(1),\mathcal{N}]\subset t^{c_0}\widetilde{\mathcal{N}}^{(2)}$);

d) $\mathcal{R}(\mathcal{N}(2)+t^{c_0}\widetilde{\mathcal{N}}^{(2)})\subset\mathcal{N}(2)+t^{c_0}\widetilde{\mathcal{N}}^{(2)}$, $\mathcal{R}(\tilde{e}-e-e_1^-)=\tilde{e}-e-e_1^-$, $\mathcal{R}(c^0-\sigma c^0+e_1^+)=0$ and, therefore, c) implies that

$$\tilde{e}\equiv e+e_1^-\bmod\mathcal{N}(2)+t^{c_0}\widetilde{\mathcal{N}}^{(2)}$$

or, more explicitly,

$$\tilde{e}\equiv\sum_{a\in\mathbb{Z}^+(p)}t^{-a}\left(D_{a0}-a\sum_{i\geqslant 0}\alpha_i(h)D_{a+c_0+pi,0}\right)+\alpha_0D_0\bmod\mathcal{N}(2)+t^{c_0}\widetilde{\mathcal{N}}^{(2)}\,.$$

It remains to prove that this congruence is equivalent to the statement of our lemma. Note that any element $l\in\mathcal{L}_{\mathcal{K}}$ can be uniquely presented as $l=\sum_{b\in\mathbb{Z}}t^bl_b$, where all $l_b\in\mathcal{L}_k$ and $l_b\to 0$ if $b\to-\infty$.

Suppose $s\geqslant 1$ and $-(s-1)c_0\geqslant b>-sc_0$.

Then it follows directly from definitions that:

— if $l \in \mathcal{N}$ then $l_b \in \mathcal{L}(s)_k$;

— if $l \in \mathcal{N}(2)$ then $l_b \in \mathcal{L}(s+2)_k$;

— if $l \in t^{c_0}\widetilde{\mathcal{N}}^{(2)}$ then $l_b \in \mathcal{L}(s+1)_k \cap C_2(\mathcal{L}_k)$.

It remains to compare the coefficients in the last congruence for $\tilde{e}$. □

2.5. **The group $\mathcal{G}_h$.** Let

$$\mathcal{M} := \mathcal{N} + \mathcal{L}(p)_{\mathcal{K}} = \sum_{1 \leqslant s < p} t^{-sc_0}\mathcal{L}(s)_{\mathrm{m}} + \mathcal{L}(p)_{\mathcal{K}}$$

$$\mathcal{M}_{<p} := \sum_{1 \leqslant s < p} t^{-sc_0}\mathcal{L}(s)_{\mathrm{m}_{<p}} + \mathcal{L}(p)_{\mathcal{K}_{<p}}$$

where $\mathrm{m}_{<p}$ is the maximal ideal of the valuation ring of $\mathcal{K}_{<p}$.

Then $\mathcal{M}$ has the induced structure of a Lie $\mathbb{F}_p$-algebra (use the Lie bracket from $\mathcal{L}_{\mathcal{K}}$) and for $i \geqslant 0$, $\mathcal{M}(i) := t^{ic_0}\mathcal{M}$ is a decreasing filtration of ideals in $\mathcal{M}$. Note that $e \in \mathcal{M}$. Similarly, $\mathcal{M}_{<p}$ is a Lie $\mathbb{F}_p$-algebra (containing $\mathcal{M}$ as its subalgebra) and for $i \geqslant 0$, $\mathcal{M}_{<p}(i) := t^{ic_0}\mathcal{M}_{<p}$ is a decreasing filtration of ideals in $\mathcal{M}_{<p}$, $\mathcal{M}_{<p}(i) \cap \mathcal{M} = \mathcal{M}(i)$.

There is a natural embedding of $\bar{\mathcal{M}} := \mathcal{M}/\mathcal{M}(p-1)$ into $\bar{\mathcal{M}}_{<p} := \mathcal{M}_{<p}/\mathcal{M}_{<p}(p-1)$, and the induced decreasing filtrations of ideals $\bar{\mathcal{M}}(i)$ and $\bar{\mathcal{M}}_{<p}(i)$ (where $\bar{\mathcal{M}}(p-1) = \bar{\mathcal{M}}_{<p}(p-1) = 0$) are compatible with this embedding. Note that for all $i \geqslant 0$, $(\mathrm{id}_{\mathcal{L}} \otimes h - \mathrm{id}_{\mathcal{M}})^i\mathcal{M} \subset \mathcal{M}(i)$.

**Lemma 2.7.** $f, \sigma f \in \mathcal{M}_{<p}$.

*Proof.* Prove by induction on $1 \leqslant s \leqslant p$ that $f, \sigma f \in \mathcal{M}_{<p} + \mathcal{L}(s)_{\mathcal{K}_{<p}}$.

If $s = 1$ then $f \in \mathcal{L}_{\mathcal{K}_{<p}} = \mathcal{M}_{<p} + \mathcal{L}(1)_{\mathcal{K}_{<p}}$.

Suppose $1 \leqslant s_0 < p$ and $f, \sigma f \in \mathcal{M}_{<p} + \mathcal{L}(s_0)_{\mathcal{K}_{<p}}$.

For $1 \leqslant s \leqslant s_0 + 1$ let $j_s = \mathrm{rk}_{\mathbb{F}_p}(\mathcal{L}/\mathcal{L}(s))$. Then $0 = j_1 < j_2 < \cdots < j_{s_0+1}$. Let $l_1, \ldots, l_{j_{s_0+1}} \in \mathcal{L}$ be such that for all $1 \leqslant s \leqslant s_0 + 1$, $l_{j_s+1}, \ldots, l_{j_{s_0+1}}$ give an $\mathbb{F}_p$-basis of $\mathcal{L}(s)$ modulo $\mathcal{L}(s_0+1)$. This means that for all such $s$, the elements $l_{j_s+1}, \ldots, l_{j_{s+1}}$ form $\mathbb{F}_p$-basis of $\mathcal{L}(s)$ modulo $\mathcal{L}(s+1)$.

With above notation for $1 \leqslant j \leqslant j_{s_0+1}$, there are unique $b_j \in \mathcal{K}_{<p}$ such that $f \equiv \sum_j b_j l_j \bmod \mathcal{L}(s_0+1)_{\mathcal{K}_{<p}}$. By inductive assumption, if $s < s_0$ and $l_j \in \mathcal{L}(s) \setminus \mathcal{L}(s+1)$ then $b_j, \sigma b_j \in \mathrm{m}_{<p}t^{-c_0 s}$ and we must prove that if $l_j \in \mathcal{L}(s_0)$ then $b_j \in \mathrm{m}_{<p}t^{-c_0 s_0}$.

Let $e \circ f = e + f + X(f,e)$. Then $X(f,e) \in \mathcal{M}_{<p} + \mathcal{L}(s_0+1)_{\mathcal{K}_{<p}}$ (use that $e \in \mathcal{M}_{<p}$ and $[\mathcal{M}_{<p}, \mathcal{L}(s_0)_{\mathcal{K}_{<p}}] \subset \mathcal{L}(s_0+1)_{\mathcal{K}_{<p}}$) and, therefore, $\sigma f - f \in \mathcal{M}_{<p} + \mathcal{L}(s_0+1)_{\mathcal{K}_{<p}}$.

Thus, $\sigma f - f \equiv \sum_j a_j l_j$, where for all $s \leqslant s_0$ and $j_s < j \leqslant j_{s+1}$, we have $a_j \in \mathrm{m}_{<p}t^{-c_0 s}$. In particular, for the indices $j_{s_0} < j \leqslant j_{s_0+1}$, we have $\sigma b_j - b_j \in \mathrm{m}_{<p}t^{-c_0 s_0}$. Therefore,

$$\sigma(b_j t^{c_0 s_0/p}) - t^{c_0 s_0(1-1/p)}(b_j t^{c_0 s_0/p}) \in \mathrm{m}_{<p}\,,$$

and this implies that $b_j t^{c_0 s_0/p} \in \mathrm{m}_{<p}$ and $\sigma b_j, b_j \in \mathrm{m}_{<p} t^{-c_0 s_0}$. Lemma 2.7 is proved. $\square$

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

**Proposition 2.8.** *Exact sequence* (2.3) *induces the following exact sequence of p-groups*

$$1 \longrightarrow G(\mathcal{L})/G(\mathcal{L}(p)) \longrightarrow \mathcal{G}_h \longrightarrow \langle h \rangle \bmod \langle h^p \rangle \longrightarrow 1 \tag{2.5}$$

*Proof.* Consider the orbit of $\bar{f} := f \bmod \mathcal{M}_{<p}(p-1)$ with respect to the natural action of $\widetilde{\mathcal{G}}_h \subset \mathrm{Aut}\, \mathcal{K}_{<p}$ on $\bar{\mathcal{M}}_{<p}$. Then the stabilizer $\mathcal{H}$ of $\bar{f}$ equals $\widetilde{\mathcal{G}}_h^p C_p(\widetilde{\mathcal{G}}_h)$. This fact and the remaining part of the proof appear as just a special case of the proof of Proposition 3.5 in [7]. $\square$

**Corollary 2.9.** *If $L_h$ is a Lie algebra over $\mathbb{F}_p$ such that $\mathcal{G}_h = G(L_h)$ then* (2.5) *induces the exact sequence of Lie $\mathbb{F}_p$-algebras*

$$0 \longrightarrow \bar{\mathcal{L}} (= \mathcal{L}/\mathcal{L}(p)) \longrightarrow L_h \longrightarrow \mathbb{F}_p h \longrightarrow 0\,.$$

## 3. Structure of $L_h$

Recall that we use the notation $h_{<p}$ for arbitrary lifts of $h$ to $\mathcal{K}_{<p}$, in particular, we do not require that $h_{<p}$ coincides with $h^0_{<p}$ from the end of Subsection 2.3. We will use the notation $\mathcal{K}(p) := \mathcal{K}_{<p}^{G(\mathcal{L}(p))}$ and $h(p) := h_{<p}|_{\mathcal{K}(p)}$. Because $G(\mathcal{L}(p)) = C_p(\widetilde{\mathcal{G}}_h)$ the elements of $\widetilde{\mathcal{G}}_h$ map $\mathcal{K}(p)$ to itself and we have a natural inclusion $\widetilde{\mathcal{G}}_h/G(\mathcal{L}(p)) \subset \mathrm{Aut}\mathcal{K}(p)$. The conjugations $\mathrm{Ad}\, h(p)$ on $G(\bar{\mathcal{L}}) \subset \widetilde{\mathcal{G}}_h/G(\mathcal{L}(p))$ allow us to recover the group structure on $\widetilde{\mathcal{G}}_h/G(\mathcal{L}(p))$. There are also induced conjugations (still denoted by $\mathrm{Ad}h(p)$) on $\mathcal{G}_h = \widetilde{\mathcal{G}}_h/\widetilde{\mathcal{G}}_h^p G(\mathcal{L}(p))$ which can be used as well to study the structure of the group $\mathcal{G}_h$ and its Lie algebra $L_h$ from Corollary 2.9.

The conjugations $\mathrm{Ad}\, h(p)$ appear as unipotent automorphisms of the Lie algebra $\bar{\mathcal{L}}$ and we can introduce a differentiation $\mathrm{ad}\, h(p)$ of $\bar{\mathcal{L}}$ by the relation $\mathrm{Ad}\, h(p) = \widetilde{\exp}(\mathrm{ad}\, h(p))$, where $\widetilde{\exp}$ is the truncated exponential, cf. Subsection 2.1. So, the knowledge of the Lie algebra $L_h$ is equivalent to the knowledge of the differentiation $\mathrm{ad}\, h(p)$. The lift $h(p)$ of $h$ can be fully desribed via the nilpotent Artin-Schreier theory by the use of the element $f \bmod \mathcal{L}(p)_{\mathcal{K}_{<p}} \in \bar{\mathcal{L}}_{\mathcal{K}(p)}$. As a matter of fact, the identification $\mathrm{Gal}(\mathcal{K}(p)/\mathcal{K}) \simeq G(\bar{\mathcal{L}})$ is given by the correspondence $\tau \mapsto (-\bar{f}) \circ \tau(\bar{f})$, where $\bar{f} = f \bmod \mathcal{M}_{<p}(p-1)$, and the natural identification $\bar{\mathcal{L}} = \bar{\mathcal{M}}_{<p}|_{\sigma=\mathrm{id}}$.

3.1. **Interpretation of the action of $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h$ on $\bar{\mathcal{M}}$.** Consider the induced action of $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h$ on $\bar{\mathcal{M}}$ (and agree to use for this action the same notation). Recall that $h(t) = tE(\omega_h^p)$, where

$$\omega_h^p = \sum_{i \geqslant 0} A_i(h) t^{c_0 + pi}$$

with all $A_i(h) \in k$, $A_0(h) \neq 0$, cf. Subsection 2.1.

Let $\mathcal{H}$ be a linear continuous operator on $\mathcal{L}_\mathcal{K}$ such that for all $a \in \mathbb{Z}$ and $l \in \mathcal{L}_k$, $\mathcal{H}(t^a l) = at^a \omega_h^p l$. Then on $\bar{\mathcal{M}}$ we have $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h = \widetilde{\exp}(\mathcal{H})$ (use that $\mathcal{H}^p = 0$ on $\bar{\mathcal{M}}$ and $E(X) \equiv \widetilde{\exp}(X) \bmod \deg p$).

Set for $0 \leqslant i < p$, $h_i := \mathcal{H}^i/i! : \bar{\mathcal{M}} \longrightarrow \bar{\mathcal{M}}$ and for $i \geqslant p$, $h_i = 0$. Then for any $j \geqslant 0$, $h_i(\bar{\mathcal{M}}(j)) \subset \bar{\mathcal{M}}(i+j)$ and for any natural $n$, $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h)^n = \sum_{i \geqslant 0} n^i h_i$. An analogue of these properties appears below when we study the action of $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$ on $\bar{f} \in \bar{\mathcal{M}}_{<p}$.

3.2. **General situation.** The situation from Subsection 3.1 can be formalized as follows.

Suppose $\mathfrak{M}$ is an $\mathbb{F}_p$-module (actually we can assume that $\mathfrak{M}$ is a module over any ring where $(p-1)!$ is invertible). Suppose $g : \mathfrak{M} \longrightarrow \mathfrak{M}$ is an automorphism of $\mathfrak{M}$ such that $g^p = \mathrm{id}_\mathfrak{M}$. Assume that

• *for any $m \in \mathfrak{M}$, there are $g_i(m) \in \mathfrak{M}$, where $1 \leqslant i < p$, such that for all $n \geqslant 0$, $g^n(m) = m + \sum_{1 \leqslant i < p} g_i(m) n^i$.*

Set $g_0(m) = m$ and $g_i(m) = 0$ if $i \geqslant p$.

**Proposition 3.1.** *With above notation we have:*

a) *for all $i \geqslant 0$, $g_i : \mathfrak{M} \longrightarrow \mathfrak{M}$ are unique linear morphisms;*

b) *for all $i \geqslant 0$, $g_i(\mathfrak{M}) \subset (g - \mathrm{id}_\mathfrak{M})^i(\mathfrak{M})$;*

c) *if $i_1, \ldots, i_s \geqslant 0$ then $(g_{i_1} \cdot \ldots \cdot g_{i_s})(\mathfrak{M}) \subset (g - \mathrm{id}_\mathfrak{M})^{i_1 + \cdots + i_s}(\mathfrak{M})$;*

d) *the map $g^U = \sum_{i \geqslant 0} g_i \otimes U^i : \mathfrak{M} \longrightarrow \mathfrak{M} \otimes \mathbb{F}_p[[U]]$ determines the action of the formal additive group $\mathbb{G}_a = \operatorname{Spf} \mathbb{F}_p[[U]]$ on $\mathfrak{M}$;*

e) *if $1 \leqslant i < p$ then $g_i = g_1^i/i!$ (here $g_1^i = \underbrace{g_1 \cdot \ldots \cdot g_1}_{i \text{ times}}$).*

*Proof.* For any $m \in \mathfrak{M}$, $g_1(m), \ldots, g_{p-1}(m)$ are unique solutions of the non-degenerate system of equations

$$\sum_{1 \leqslant i < p} g_i(m) n^i = g^n(m) - m$$

where $n = 1, \ldots, p-1$. Therefore, all $g_i(m)$ are unique and depend linearly on $m$. This proves a).

For $i \geqslant 0$ and $F \in \mathfrak{M} \otimes \mathbb{F}_p[[U]]$, define the $i$-th differences $(\Delta^i F)(U) \in \mathfrak{M} \otimes \mathbb{F}_p[[U]]$ by setting $\Delta^0 F = F$ and

$$(\Delta^{i+1} F)(U) = (\Delta^i F)(U+1) - (\Delta^i F)(U).$$

In particular, for $0 \leqslant j < i$, $\Delta^i(m \otimes U^j) = 0$ and $(\Delta^i)(m \otimes U^i) = i! m$. Therefore, for any $i \geqslant 0$,

$$(\Delta^i g^U(m))|_{U=0} = i! g_i(m) + \sum_{j > i} f_{ij} g_j(m), \tag{3.1}$$

where all $f_{ij} \in \mathbb{F}_p$. Note that for every value $n_0 \geqslant 0$,

$$(\Delta^1 g^U)(m)|_{u=n_0} = g(g^U(m)|_{u=n_0}) - g^U(m)|_{u=n_0} \in (g - \mathrm{id}_{\mathfrak{M}})(\mathfrak{M}),$$

$(\Delta^2 g^U)(m)|_{u=n_0} = g((\Delta^1 g^U)(m)|_{u=n_0}) - (\Delta^1 g^U)(m)|_{u=n_0} \in (g - \mathrm{id}_{\mathfrak{M}})^2(\mathfrak{M})$ and so on. Therefore, for any $i \geqslant 0$,

$$(\Delta^i g^U)(m)|_{U=n_0} \in (g - \mathrm{id}_{\mathfrak{M}})^i \mathfrak{M}\,.$$

Then (3.1) implies (use $i = p-1$) that $g_{p-1}(m) \in (g - \mathrm{id}_{\mathfrak{M}})^{p-1}(\mathfrak{M})$ and then by descending induction on $i$ that $g_i(m) \in (g - \mathrm{id}_{\mathfrak{M}})^i(\mathfrak{M})$. This proves b).

In c) use induction on $s$. The case $s = 1$ is proved in b). If $s > 1$ then we must prove with $j = i_2 + \ldots i_s$ that

$$g_{i_1}((g - \mathrm{id}_{\mathfrak{M}})^j \mathfrak{M}) \subset (g - \mathrm{id}_{\mathfrak{M}})^{i_1 + j} \mathfrak{M}\,.$$

This can be obtained from a) by replacing $\mathfrak{M}$ to $(g - \mathrm{id}_{\mathfrak{M}})^j \mathfrak{M}$.

For any natural numbers $n_1, n_2$ the relation $g^{n_1+n_2}(m) = g^{n_2}(g^{n_1}(m))$ means that

$$\sum_{0 \leqslant i < p} (n_1 + n_2)^i g_i = \sum_{0 \leqslant i_1, i_2 < p} n_2^{i_2} n_1^{i_1} g_{i_2} \circ g_{i_1}\,,$$

and implies that we have the appropriate identity of formal power series

$$(g^U \otimes \mathrm{id}_{\mathbb{G}_a}) \circ g^U = (\mathrm{id}_{\mathfrak{M}} \otimes \Delta_{\mathbb{G}_a}) \circ g^U\,,$$

with the coaddition $\Delta = \Delta_{\mathbb{G}_a}$ in $\mathbb{G}_a$ such that $\Delta(U) = U \otimes 1 + 1 \otimes U$. This proves d).

If $i \geqslant 1$ the above identity for $g^U$ implies the identity

$$(g^U \otimes \mathrm{id}_{\mathbb{G}_a^i}) \circ \cdots \circ (g^U \otimes \mathrm{id}_{\mathbb{G}_a}) \circ g^U = (\mathrm{id}_{\mathfrak{M}} \otimes \Delta^{(i)}) \circ g^U\,,$$

where $\Delta^{(i)} = (\Delta \otimes \mathrm{id}_{\mathbb{G}_a^{i-1}}) \circ \cdots \circ (\Delta \otimes \mathrm{id}_{\mathbb{G}_a}) \circ \Delta$ is the $i$-th coaddition $\mathbb{F}_p[[U]] \longrightarrow \mathbb{F}_p[U]^{\otimes i}$ for $\mathbb{G}_a$. Then e) can be obtained by compairing the coefficients for $U^{\otimes i}$ in this identity. □

**Definition.** $dg^U := g_1 \otimes U : \mathfrak{M} \longrightarrow \mathfrak{M} \otimes U$ is the differential of $g$.

By Proposition 3.1e) the action of $g$ on $\mathfrak{M}$ can be uniquely recovered from its differential $dg^U$.

3.3. **Auxiliary statement.** Suppose $\mathfrak{L}$ is a finite Lie $\mathbb{F}_p$-algebra and $\mathcal{A} = \mathcal{A}(\mathfrak{L})$ is its enveloping algebra. Then there is a canonical embedding $\mathfrak{L} \longrightarrow \mathcal{A}$ and $\mathcal{A}$ can be provided with a coalgebra structure $\Delta : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$ by setting $\Delta(l) = l \otimes 1 + 1 \otimes l$ for all $l \in \mathfrak{L}$.

Let $J = J(\mathfrak{L})$ be the augmentation ideal of $\mathcal{A}$ generated by all $l \in \mathfrak{L}$. Note that $\mathcal{A} \otimes \mathcal{A}$ can be identified with the enveloping algebra of $\mathfrak{L} \oplus \mathfrak{L}$ and the appropriate augmentation ideal equals $J(\mathfrak{L} \oplus \mathfrak{L}) = J \otimes \mathcal{A} + \mathcal{A} \otimes J$.

Suppose $\mathfrak{L}$ has nilpotent class $< p$. Then we have the following interpretation of the Campbell-Hausdorff operation $\circ$ on $\mathfrak{L}$ in the envelopping algebra $\mathcal{A}$:

$\alpha)$ $\mathfrak{L} = \{a \in \mathcal{A} \bmod J(\mathfrak{L})^p \mid \Delta a \equiv a \otimes 1 + 1 \otimes a \bmod J(\mathfrak{L} \oplus \mathfrak{L})^p\}$;

$\beta$) the truncated exponential $\widetilde{\exp}$ establishes a group isomorphism $\iota : G(\mathfrak{L}) \longrightarrow \mathcal{D}(\mathfrak{L})$, where

$$\mathcal{D}(\mathfrak{L}) = \{a \in 1 + J(\mathfrak{L}) \bmod J(\mathfrak{L})^p \mid \Delta a \equiv a \otimes a \bmod J(\mathfrak{L} \oplus \mathfrak{L})^p\}$$

is the group of " diagonal elements of $\mathcal{A}$ modulo degree $p$" with respect to the operation induced by the multiplication in $\mathcal{A}$;

$\gamma$) $\iota^{-1} : \mathcal{D}(\mathfrak{L}) \longrightarrow G(\mathfrak{L})$ is given via the truncated logarithm $\widetilde{\log}$.

Let $l_1, \dots, l_r$ be an $\mathbb{F}_p$-basis of $\mathfrak{L}$. Then by the Poincare-Birkhoff-Witt Theorem, $\mathcal{B}_1 = \{l_{i_1} \dots l_{i_s} \mid s \geqslant 0,\, i_1 \leqslant \dots \leqslant i_s\}$ is an $\mathbb{F}_p$-basis of $\mathcal{A}$ and $\mathcal{A} \bmod J(\mathfrak{L})^p$ can be identified with the submodule $\mathcal{M}_1$ of $\mathcal{A}$ generated by the elements of $\mathcal{B}_1^{<p} := \{l_{i_1} \dots l_{i_s} \in \mathcal{B}_1 \mid s < p\}$.

For similar reasons, use the basis $\{(l_i, 0), (0, l_i) \mid 1 \leqslant i \leqslant r\}$ of $\mathfrak{L} \oplus \mathfrak{L}$ to construct the $\mathbb{F}_p$-basis for $\mathcal{A} \otimes \mathcal{A}$ in the form

$$\mathcal{B}_2 = \{l_{i_1} \dots l_{i_s} \otimes l_{j_1} \dots l_{j_t} \mid s, t \geqslant 0,\, i_1 \leqslant \dots \leqslant i_s,\, j_1 \leqslant \dots \leqslant j_t\}\,.$$

Then $\mathcal{A} \otimes \mathcal{A} \bmod J(\mathfrak{L} \oplus \mathfrak{L})^p$ can be identified with the module $\mathcal{M}_2$ generated by the subset $\mathcal{B}_2^{<p}$ of $\mathcal{B}_2$ consisting of elements with $s+t < p$.

Let $\delta^+ = \Delta - \mathrm{id}_{\mathcal{A}} \otimes 1 - 1 \otimes \mathrm{id}_{\mathcal{A}}$. Then $\delta^+(\mathcal{M}_1) \subset \mathcal{M}_2$ and it is easy to see that:

- $\mathfrak{L} \subset \operatorname{Ker} \delta^+$;
- if $l \in \mathcal{B}_1^{<p} \setminus \mathfrak{L}$ then $l \notin \operatorname{Ker} \delta^+$;
- if $l', l'' \in \mathcal{B}_1^{<p} \setminus \mathfrak{L}$ then $\delta^+(l')$ and $\delta^+(l'')$ are linear combinations of disjoint groups of elements of $\mathcal{B}_2^{<p}$.

In other words, we have a direct sum of non-zero submodules

$$\delta^+(\mathcal{M}_1) = \bigoplus_{l \in \mathcal{B}_1^{<p} \setminus \mathfrak{L}} \mathbb{F}_p \delta^+(l)\,.$$

The above facts prove $\alpha$). The verification of $\beta$) and $\gamma$) is formal.

In this paper we are dealing with more elaborate situation.

Suppose $\mathfrak{L}$ is provided with a decreasing filtration of ideals $\{\mathfrak{L}^i\}_{i \geqslant 0}$ such that $\mathfrak{L}^0 = \mathfrak{L}$ and $\mathfrak{L}^i = 0$ if $i \geqslant p$. Define the weight function on $\mathfrak{L}$ by setting $\mathrm{wt}^*(0) = \infty$ and $\mathrm{wt}^*(l) = i$ if $l \in \mathfrak{L}^i \setminus \mathfrak{L}^{i+1}$.

Assume in addition that the filtration $\{\mathfrak{L}^i\}$ is "central", i.e. for any $i, j \geqslant 0$, $[\mathfrak{L}^i, \mathfrak{L}^j] \subset \mathfrak{L}^{i+j}$.

Suppose the $\mathbb{F}_p$-basis $\{l_i \mid 1 \leqslant i \leqslant r\}$ of $\mathfrak{L}$ is compatible with the filtration $\{\mathfrak{L}^i\}_{i \geqslant 0}$, i.e. there are $0 = j_0 \leqslant j_1 \leqslant \dots \leqslant j_p = r$ such that for any $i \geqslant 0$, $\{l_j \mid j_i < j \leqslant r\}$ is an $\mathbb{F}_p$-basis of $\mathfrak{L}^i$. Use again $\mathcal{B}_1$ as a basis of $\mathcal{A}$ over $\mathbb{F}_p$. Extend $\mathrm{wt}^*$ to $\mathcal{A}$ by setting for every non-zero $\mathbb{F}_p$-linear combination,

$$\mathrm{wt}^*\left(\sum_{i_1, \dots, i_s} \alpha_{i_1 \dots i_s} l_{i_1} \dots l_{i_s}\right) = \min\{\mathrm{wt}^*(l_{i_1}) + \dots + \mathrm{wt}^*(l_{i_s}) \mid \alpha_{i_1 \dots i_s} \neq 0\}\,.$$

Let $\mathcal{A}^i = \{a \in \mathcal{A} \mid \mathrm{wt}^*(a) \geqslant i\}$. Then for any $i, j \geqslant 0$, $\mathcal{A}^i\mathcal{A}^j \subset \mathcal{A}^{i+j}$ (use that $\{\mathfrak{L}^i\}$ is "central"). In particular, $\{\mathcal{A}^i\}_{i\geqslant 0}$ is a decreasing filtration of ideals of $\mathcal{A}$. Obviously, $\mathcal{A}^i \cap \mathfrak{L} = \mathfrak{L}^i$.

Let $B$ be a $\mathbb{Z}_p$-linear operator on $\mathfrak{L}$ such that for any $l \in \mathfrak{L}^i$, $B(l) \equiv l \bmod \mathfrak{L}^{i+1}$. For $l \in \mathfrak{L}$ and $n \in \mathbb{N}$, set in the appropriate $p$-group $G(\mathfrak{L})$, $l[n] := l \circ B(l) \circ \cdots \circ B^{n-1}(l)$.

**Proposition 3.2.** *Suppose $l \in \mathfrak{L}^1$. For $1 \leqslant i \leqslant p-1$ there are (unique) $l_i \in \mathfrak{L}^i$ such that for any $n \geqslant 0$, $l[n] = l_1 n + l_2 n^2 + \cdots + l_{p-1} n^{p-1}$.*

*Proof.* Prove the existence of $l_i \in \mathfrak{L}^i$. (For the uniqueness of $l_i$, proceed similarly to Proposition 3.1a).)

Clearly, $B = \widetilde{\exp}(\mathcal{B})$, where $\mathcal{B}$ is a linear operator on $\mathfrak{L}$ such that for all $i$, $\mathcal{B}(\mathfrak{L}^i) \subset \mathfrak{L}^{i+1}$. If for $0 \leqslant i \leqslant p-1$, $l'_i = \mathcal{B}^i(l)/i!$ then $l'_i \in \mathfrak{L}^{i+1}$ and for any $m \geqslant 0$, $B^m(l) = \widetilde{\exp}(m\mathcal{B})(l) = \sum_{i\geqslant 0} l'_i m^i$. (We set $0^0 = 1$.)

Let $\mathcal{E} : \mathfrak{L} \longrightarrow \mathcal{A}$ be the map given by the truncated exponential. Then for $i \geqslant 0$, there are $d_i \in \mathcal{A}^{i+1}$ such that for any $m \geqslant 0$,

$$\mathcal{E}(B^m(l)) = 1 + \sum_{i\geqslant 0} d_i m^i \,.$$

Therefore, $\mathcal{E}(l)\mathcal{E}(B(l)) \dots \mathcal{E}(B^{n-1}(l)) =$

$$1 + \sum_{\substack{1\leqslant s<n \\ i_1,\dots,i_s\geqslant 0}} \left( \sum_{0\leqslant m_1<\cdots<m_s<n} m_1^{i_1} \dots m_s^{i_s} \right) d_{i_1} \dots d_{i_s} \,.$$

Let $d(i_1, \dots, i_s) := i_1 + \cdots + i_s + s$ and

$$\sum_{0\leqslant m_1<\cdots<m_s<n} m_1^{i_1} \dots m_s^{i_s} = f_{i_1\dots i_s}(n) \,.$$

Note that $d_{i_1} \dots d_{i_s} \in \mathcal{A}^{d(i_1,\dots,i_s)}$.

**Lemma 3.3.** *If $s \geqslant 1$, $i_1, \dots, i_s \geqslant 0$ and $d(i_1, \dots, i_s) < p$ then there are polynomials $F_{i_1\dots i_s} \in \mathbb{Z}_p[U]$ such that:*

a) *for all $n$, $F_{i_1\dots i_s}(n) = f_{i_1\dots i_s}(n)$;*

b) *$F_{i_1\dots i_s}(0) = 0$;*

c) *$\deg F_{i_1\dots i_s} = d(i_1, \dots, i_s)$.*

*Proof of Lemma.* First, consider the case $s = 1$.

Apply induction on $i_1$.

If $i_1 = 0$ then $f_0(n) = n$ and we can take $F_0 = U$.

Suppose $i_1 \geqslant 1$, $d(i_1) < p$ (i.e. $0 \leqslant i_1 \leqslant p-2$) and our Lemma is proved for all indices $j < i_1$.

For any $m < n$ we have,

$$(m+1)^{i_1+1} - m^{i_1+1} = \sum_{0\leqslant j\leqslant i_1} C_j(i_1) m^j \,,$$

where all $C_j(i) \in \mathbb{Z}_p$. Therefore, for any $n \geqslant 0$,

$$n^{i_1+1} = \sum_{0 \leqslant j \leqslant i_1} C_j(i_1) f_j(n) = \sum_{0 \leqslant j < i_1} C_j(i_1) F_j(n) + (i_1+1) f_{i_1}(n)$$

and we can take as $F_{i_1}(U)$ the polynomial

$$\frac{1}{i_1+1}\left(U^{i_1+1} - \sum_{0 \leqslant j < i_1} C_j(i_1) F_j(U)\right) = \sum_{j \leqslant i_1+1} A_j(i_1) U^j \in \mathbb{Z}_p[U]\,.$$

Clearly, the degree of $F_{i_1}$ equals $i_1 + 1 = d(i_1)$ and $F_{i_1}(0) = 0$. The case $s = 1$ is considered.

Suppose $s > 1$ and use induction on $s$. Then for any $m < n$,

$$f_{i_1 \dots i_s}(m+1) - f_{i_1 \dots i_s}(m) = \sum_{0 \leqslant m_1 < \dots < m_s = m} m_1^{i_1} \dots m_s^{i_s} = m^{i_s} F_{i_1 \dots i_{s-1}}(m)\,.$$

By the inductive assumption we have

$$F_{i_1 \dots i_{s-1}}(U) = \sum_{j \leqslant d(i_1, \dots, i_{s-1})} A_j(i_1, \dots, i_{s-1}) U^j \in \mathbb{Z}_p[U]\,.$$

Then for any $n \geqslant 1$ (note that $d(i_1, \dots, i_s) - 1 = d(i_1, \dots, i_{s-1}) + i_s$),

$$f_{i_1 \dots i_s}(n) = \sum_{i_s \leqslant j \leqslant d(i_1, \dots, i_s) - 1} A_{j - i_s}(i_1, \dots, i_{s-1}) F_j(n)\,,$$

and we can take $F_{i_1 \dots i_s} = \sum_{i_s \leqslant j \leqslant d(i_1, \dots, i_s)-1} A_{j-i_s}(i_1, \dots, i_{s-1}) F_j$. Clearly, the degree of $F_{i_1 \dots i_s}$ equals $d(i_1, \dots, i_s)$ and $F_{i_1 \dots i_s}(0) = 0$. □

The above lemma implies that for all $n \geqslant 1$,

$$\mathcal{E}(l[n]) = 1 + \sum_{1 \leqslant i \leqslant p-1} d'_i n^i + a(l, n)\,,$$

where all $d'_i \in \mathcal{A}^i$ and $a(l, n) \in \mathcal{A}^p$ (recall that $\mathcal{A}^p \supset J(\mathfrak{L})^p$).

Applying to this equality the truncated logarithm we obtain that $l[n] = d''_1 n + \dots + d''_{p-1} n^{p-1} + b(l, n)$, where all $d''_i \in \mathcal{A}^i$ and $b(l, n) \in \mathcal{A}^p$. Therefore, for all $1 \leqslant n \leqslant p-1$, we have $d''_1 n + \dots + d''_{p-1} n^{p-1} \in \mathfrak{L} + \mathcal{A}^p$. This implies that all $d''_i \in \mathfrak{L} + \mathcal{A}^p$ (use that $\det(n^i)_{1 \leqslant n, i < p} \not\equiv 0 \bmod p$), i.e. $d''_i \in \mathcal{A}^i \cap (\mathfrak{L} + \mathcal{A}^p) = \mathfrak{L}^i + \mathcal{A}^p$ (use that for $0 \leqslant i < p$, $\mathcal{A}^i \cap \mathfrak{L} = \mathfrak{L}^i$). Finally, if $l_i \in \mathfrak{L}$ are such that $d''_i - l_i \in \mathcal{A}^p$ then

$$l[n] - (l_1 n + l_2 n^2 + \dots + l_{p-1} n^{p-1}) \in \mathfrak{L} \cap \mathcal{A}^p = 0\,.$$

The proposition is proved. □

As a matter of fact, the proof of Proposition 3.2 gives the following result:

• *If $i^0 \geqslant 1$ and $l \in \mathfrak{L}^{i^0}$ then for $1 \leqslant i \leqslant p - i^0$ there are unique $l_i \in \mathfrak{L}^{i+i^0-1}$ such that for any $n \geqslant 0$, $l[n] = l_1 n + \dots + l_{p-i^0} n^{p-i^0}$.*

We should formally follow the above proof of Proposition 3.1. Then $l \in \mathfrak{L}^{i_0}$ implies that all $l'_i \in \mathfrak{L}^{i+i_0}$, $d_i \in \mathcal{A}^{i+i_0}$. Lemma 3.3 remains

unchanged and, finally, all $d_i' \in \mathcal{A}^{i+i_0-1}$ and all $l_i \in \mathcal{A}^{i+i^0-1} \cap \mathfrak{L} = \mathfrak{L}^{i+i_0-1}$ if $i \leqslant p - i_0$.

This allows us to state the following result.

**Proposition 3.4.** *There are linear maps $\pi_i : \mathfrak{L}^1 \longrightarrow \mathfrak{L}^1$ such that for any $j \geqslant 0$, $\pi_i(\mathfrak{L}^j) \subset \mathfrak{L}^{i+j-1}$ (in particular, $\pi_i = 0$ if $i \geqslant p$) and for any $l \in \mathfrak{L}^1$ and $n \in \mathbb{N}$, $l[n] = \sum_i \pi_i(l) n^i$.*

3.4. **Lie algebra $\bar{\mathcal{M}}^f$ and the action of $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$.** Here we study the action of $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$ on $\bar{f} = f \bmod \mathcal{M}_{<p}(p-1) \in \bar{\mathcal{M}}_{<p}$.

Note that if $h^0_{<p}$ is the lift from the end of Subsection 2.3 then $h^0_{<p}(f) = c^0 \circ (\mathrm{Ad}\, h^0_{<p} \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$, where $c^0 \in \mathcal{N}(1) \subset \mathcal{M}(1)$, cf. the proof of Lemma 2.6 step b).

Suppose $h_{<p}$ is any lift of $h$. Then there is $l \in \mathcal{L} = \mathcal{L}(1)$ such that $h_{<p} = h^0_{<p}\eta_0^{-1}(l)$: if $(\mathrm{id}_{\mathcal{L}} \otimes h_{<p})f = c \circ (A \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$ then by Proposition 2.3, $c = c^0 \circ l \in \mathcal{L}(1)_k + \mathcal{M}(1)$. In other words, generally $c \notin \mathcal{N}(1)$ but it always belongs to $\mathcal{L}(1)_k + \mathcal{M}(1) \subset \mathcal{M}$.

Proceeding in $\bar{\mathcal{M}}$ we have for $h(p) = h_{<p}|_{\mathcal{K}(p)}$,

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p))\bar{f} = \bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}\,,$$

where we set $\bar{c} = c \bmod \mathcal{M}(p-1) \in \bar{\mathcal{M}}$ and $\bar{A} = A \bmod \mathcal{L}(p) = \mathrm{Ad}\, h(p) = \widetilde{\exp}(\mathrm{ad}\, h(p))$.

For $n \in \mathbb{N}$, let

$$(\mathrm{id}_{\mathcal{L}} \otimes h^n_{<p})f = c(n) \circ f(n)\,, \tag{3.2}$$

where $c(n) = (\mathrm{id}_{\mathcal{L}} \otimes h^{n-1})(c \circ (A \otimes h^{-1})c \circ \cdots \circ (A \otimes h^{-1})^{n-1}c)$ and $f(n) = (A^n \otimes \mathrm{id}_{\mathcal{K}_{<p}})f$.

Proceeding similarly to Subsection 3.1 we obtain that

$$\bar{f}(n) := f(n) \bmod \mathcal{M}_{<p}(p-1) = \sum_{i \geqslant 0} \bar{f}^{(i)} n^i\,,$$

where $\bar{f}^{(0)} = \bar{f}$ and for all $1 \leqslant i < p$, $\bar{f}^{(i)} = (\mathrm{ad}^i h(p) \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}/i! \in (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)} - \mathrm{id}_{\bar{\mathcal{M}}_{<p}})^i \bar{\mathcal{M}}_{<p} \subset \bar{\mathcal{M}}_{<p}(i)$.

Define the new filtration $\mathcal{M}[i]$ on $\mathcal{M}$ by setting $\mathcal{M}[0] := \mathcal{M}$ and for $i \geqslant 1$, $\mathcal{M}[i] := \mathcal{L}(i)_k + \mathcal{M}(i)$. Consider the appropriate filtrations $\bar{\mathcal{M}}[i] = \mathcal{M}[i] \bmod \mathcal{M}(p-1)$ on $\bar{\mathcal{M}}$ and $\bar{\mathcal{M}}_{<p}[i] = \bar{\mathcal{M}}[i] + \bar{\mathcal{M}}_{<p}(i)$ on $\bar{\mathcal{M}}_{<p}$.

**Proposition 3.5.** *There are $c_i \in \mathcal{M}[i]$ such that for all $n \in \mathbb{N}$, $c(n) \equiv \sum_{i \geqslant 1} c_i n^i \bmod \mathcal{M}(p-1)$.*

*Proof.* Consider the Lie algebra $\mathfrak{L} = \bar{\mathcal{M}}$ with filtration $\mathfrak{L}^i := \bar{\mathcal{M}}[i]$. Clearly, $\mathfrak{L}$ and its filtration $\{\mathfrak{L}^i\}_{i \geqslant 0}$ satisfy the assumptions from Subsection 3.3 and $\bar{c} \in \mathfrak{L}^1$ (cf. the beginning of this Subsection). It remains to apply Proposition 3.2. □

**Corollary 3.6.** *For all* $n \in \mathbb{N}$,

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^n)\bar{f} = \sum_{i\geqslant 0} \bar{f}_i n^i \,,$$

*where* $\bar{f}_0 = \bar{f}$ *and all* $\bar{f}_i \in \bar{\mathcal{M}}_{<p}[i]$.

**Definition.** $\bar{\mathcal{M}}^f$ is the minimal Lie subalgebra in $\bar{\mathcal{M}}_{<p}$ containing $\bar{\mathcal{M}}$ and all the elements $(\mathrm{Ad}^n h(p) \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}$ with $n \in \mathbb{N}$.

Note that $\bar{\mathcal{M}}^f$ does not depend on a choice of the lift $h(p)$. We can also define $\bar{\mathcal{M}}^f$ as the minimal subalgebra in $\bar{\mathcal{M}}_{<p}$ containing $\bar{\mathcal{M}}$ and all $\bar{f}^{(i)}$, $1 \leqslant i < p$. Clearly, $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$ acts on $\bar{\mathcal{M}}^f$ (use that $A \otimes \mathrm{id}_{\mathcal{K}(p)}$ and $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$ commute) and this action is completely determined by the knowledge of $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p))\bar{f}$. Roughly speaking, $\bar{\mathcal{M}}^f$ is much smaller than $\bar{\mathcal{M}}_{<p}$ but it is still provided with a strict action of $\mathcal{G}_h$. In addition, the filtration $\bar{\mathcal{M}}_{<p}[i]$ induces the $\mathcal{G}_h$-equivariant filtration $\bar{\mathcal{M}}^f[i]$ on $\bar{\mathcal{M}}^f$, and for all $i$, $\bar{f}^{(i)}$ and $\bar{f}_i$ belong to $\bar{\mathcal{M}}^f[i]$.

Now we can apply the results of Subsection 3.2 and introduce the appropiate action $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U : \bar{\mathcal{M}}^f \longrightarrow \bar{\mathcal{M}}^f \otimes \mathbb{F}_p[[U]]$ of $\mathbb{G}_{a,\mathbb{F}_p}$ on $\bar{\mathcal{M}}^f$. This action appears as the extension of the action $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U : \bar{\mathcal{M}} \longrightarrow \bar{\mathcal{M}} \otimes \mathbb{F}_p[[U]]$ from Subsection 3.1 by setting

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f} = \sum_{i\geqslant 0} \bar{f}_i \otimes U^i \,.$$

By Proposition 3.1 the action of $h(p)$ is completely determined by the differential $d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)$.

3.5. **Differential** $d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)$**.** Using the calculations from Subsection 3.4 we obtain

$$\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U : \bar{f} \mapsto \bar{c}(U) \circ \bar{f}(U) \,,$$

where $\bar{c}(U) = \sum_{i\geqslant 1} c_i U^i \bmod \mathcal{M}(p-1)$ and $\bar{f}(U) = \bar{f} + \sum_{i\geqslant 1} \bar{f}^{(i)} U^i$.

Introduce the formal operator

$$\mathrm{Ad}^U h(p) : \bar{\mathcal{L}} \longrightarrow \bar{\mathcal{L}} \otimes \mathbb{F}_p[[U]]$$

such that for any $l \in \bar{\mathcal{L}} = \mathcal{L}/\mathcal{L}(p)$, $\mathrm{Ad}^U h(p) l = \sum_{i\geqslant 0} l_i U^i$, where $l_i = 0$ if $i \geqslant p$ and for any $n \in \mathbb{N}$, $\mathrm{Ad}^U h(p)|_{U=n} = \mathrm{Ad}^n h(p)$. Similarly to Subsection 3.2, for all $i \geqslant 0$, $l_i = \mathrm{ad}^i h(p)(l)/i!$ and $\mathrm{Ad}^U h(p) \equiv \mathrm{id}_{\bar{\mathcal{L}}} + \mathrm{ad} h(p)\, U \bmod U^2$. This gives the following formal identity (note $\sigma U = U$):

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U)(e) \circ \bar{c}(U) = (\sigma\bar{c})(U) \circ \sum_{a\in\mathbb{Z}^0(p)} t^{-a}(\mathrm{Ad}^U h(p) \otimes \mathrm{id}_k) D_{a0} \,. \tag{3.3}$$

The proof formally goes along the lines of the proof that $(c, A)$ satisfies identity (2.1) in Proposition 2.3.

As a result, we can specify $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f}$ by the following linearization of (3.3). Recall, cf. Subsection 2.1, that

$$h(t) = tE(\omega_h^p) \equiv t\widetilde{\exp}(\omega_h^p) \bmod t^{pc_0+1}\,,$$

where $\omega_h^p = \sum_{i \geqslant 0} A_i(h) t^{c_0+pi}$, all $A_i(h) \in k$ and $A_0(h) \neq 0$. Then by Proposition 2.1, $h^U(t) \equiv t\widetilde{\exp}(U\omega_h^p) \bmod t^{pc_0+1}$ and

$$d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U)e = -\sum_{a \in \mathbb{Z}^0(p)} t^{-a}\omega_h^p a D_{a0} \otimes U \bmod \mathcal{M}(p-1)\,.$$

**Proposition 3.7.** *We have the following recurrent congruence modulo* $\mathcal{M}(p-1)$ *for* $\bar{c}_1 = c_1 \bmod \mathcal{M}(p-1)$ *and* $V_{a0} := \mathrm{ad}\, h(p)(D_{a0}) \bmod \mathcal{L}(p)_k$, $a \in \mathbb{Z}^0(p)$,

$$\sigma\bar{c}_1 - \bar{c}_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_{a0} \equiv \tag{3.4}$$

$$-\sum_{k \geqslant 1} \frac{1}{k!}\, t^{-(a_1+\cdots+a_k)} \omega_h^p [\ldots[a_1 D_{a_1 0}, D_{a_2 0}], \ldots, D_{a_k 0}]$$

$$-\sum_{k \geqslant 2} \frac{1}{k!} t^{-(a_1+\cdots+a_k)} [\ldots[V_{a_1 0}, D_{a_2 0}], \ldots, D_{a_k 0}]$$

$$-\sum_{k \geqslant 1} \frac{1}{k!}\, t^{-(a_1+\cdots+a_k)} [\ldots[\sigma\bar{c}_1, D_{a_1 0}], \ldots, D_{a_k 0}]$$

*(the indices* $a_1, \ldots, a_k$ *in all above sums run over* $\mathbb{Z}^0(p)$*).*

*Proof.* The following properties are very well-known from the Campbell-Hausdorff theory. Suppose $X$ and $Y$ are generators of a free Lie $\mathbb{Q}[[U]]$-algebra. Then

$$(UY) \circ X \equiv X \circ \left( U \sum_{k \geqslant 0} \frac{1}{k!} [\ldots[Y, \underbrace{X], \ldots, X]}_{k \text{ times}} \right)\,,$$

$$X + UY \equiv X \circ \left( U \sum_{k \geqslant 1} \frac{1}{k!} [\ldots[Y, \underbrace{X], \ldots, X]}_{k-1 \text{ times}} \right) \bmod U^2$$

For the first formula cf. [9], Ch.II, Section 6.5 or Exercise 1 for Ch.II, Section 6. The second congruence is much more important; it can be extracted from [9], Ch.II, Section 6.5, Prop.5 or Ch.II, Exercise 3 for Section 6.

Using that the coefficients in the above formulas are $p$-integral in degrees $< p$ we can use them in the context of Lie $\mathbb{F}_p$-algebras in the following form (where $E_0(x) = (\widetilde{\exp}(x) - 1)/x$):

$$(UY) \circ X = X \circ (U\widetilde{\exp}(\mathrm{ad}X)(Y)) \bmod U^2 \tag{3.5}$$

$$X + UY = X \circ (U\, E_0(\mathrm{ad}X)(Y)) \bmod U^2 \tag{3.6}$$

**Remark.** a) In the above formulas and this paper we use the following notation: $(\mathrm{ad}X)Y = [Y, X]$ and $(\mathrm{Ad}X)Y = (-X)\circ Y \circ X$ (this notation is opposite to the notation from [9]).

b) Note the following easy rules: $X \circ (Y + U^2Z) \equiv X \circ Y \bmod U^2$ and $(UX) \circ (UY) \equiv U(X + Y) \bmod U^2$.

Then for the left-hand-side (LHS) of (3.3) modulo $U^2$ we have:

$$(e + d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U)e + \dots) \circ (\bar{c}_1 U + \dots) \equiv$$

$$e \circ E_0(\mathrm{ad}e)(d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U)e) \circ (\bar{c}_1 U + \dots) \equiv$$

$$e \circ (E_0(\mathrm{ad}e)(d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h^U)e) + \bar{c}_1 U)$$

Similarly, the RHS of (3.3) modulo $U^2$ appears in the following form

$$((\sigma\bar{c}_1)U + \dots) \circ \left( e + U \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_{a0} + \dots \right) \equiv$$

$$e \circ \left( U \sum_{a \in \mathbb{Z}^0(p)} E_0(\mathrm{ad}e)(t^{-a}V_{a0}) + U\widetilde{\exp}(\mathrm{ad}e)(\sigma\bar{c}_1) \right)$$

It remains to cancel by $e$ and equalize the coefficients for $U$. □

Any solution $\{\bar{c}_1, \{V_{a0} \mid a \in \mathbb{Z}^0(p)\}\}$ of congruence (3.4) modulo $\mathcal{M}(p-1)$ can be uniquely lifted to a solution $\{c_1, \{V_{a0} \mid a \in \mathbb{Z}^0(p)\}\}$ of (3.4) modulo $\mathcal{L}(p)_{\mathcal{K}} \subset \mathcal{M}(p-1)$. This follows easily from Lemma 2.2b) because $\sigma$ is nilpotent on $\mathcal{M}(p-1) \bmod \mathcal{L}(p)_{\mathcal{K}}$ (use that $\mathcal{M}(p-1) \subset \mathcal{L}_{\mathrm{m}} + \mathcal{L}(p)_{\mathcal{K}}$). In other words, we have a unique lift of

$$\bar{c}_1 \in \mathcal{M} \bmod \mathcal{M}(p-1) \subset \mathcal{L}_{\mathcal{K}} \bmod \mathcal{M}(p-1)$$

to $c_1 \in \mathcal{L}_{\mathcal{K}} \bmod \mathcal{L}(p)_{\mathcal{K}}$. This allows us to prove that the number of different solutions $\{\bar{c}_1, \{V_{a0} \mid a \in \mathbb{Z}^0(p)\}\}$ of (3.4) is $|\mathcal{L}/\mathcal{L}(p)|$. Indeed, we can arrange the recurrent procedure of solving congruences (3.4) modulo $\mathcal{L}(s)_{\mathcal{K}}$, where $s = 1, \dots, p$. When $s = 1$ we have only trivial solution. Then each solution modulo $\mathcal{L}(s)_{\mathcal{K}}$ gives a unique extension for all $V_a \bmod \mathcal{L}(s+1)_k$ and $|\mathcal{L}(s)/\mathcal{L}(s+1)|$ different extensions for $c_1 \bmod \mathcal{L}(s+1)_{\mathcal{K}}$. (Compare with the calculations from Subsection 2.3.) Finally, the number of different solutions of congruence (3.4) is equal to the number of different lifts of $h$ to $\mathrm{Aut}\,\mathcal{K}(p)$ which coincides with the order $|\mathrm{Gal}(\mathcal{K}_{<p}^{G(\mathcal{L}(p))}/\mathcal{K})| = |\bar{\mathcal{L}}|$. This is not very much surprising because the lift $h(p)$ is completely determined by $\bar{f}_1 U = d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U))\bar{f}$ and $\bar{f}_1$ is uniquely recovered from the knowledge of the appropriate solution $\{c_1, \{V_{a0} \mid a \in \mathbb{Z}^0(p)\}\}$ due to the following proposition 3.8 below. As a matter of fact, the above arguments give more. Suppose $c_1 = \sum_{i \in \mathbb{Z}} c_1(i)t^i$, where all $c_1(i) \in \bar{\mathcal{L}}_k$. Then different solutions $c_1$ have different $c_1(0)$, i.e. $c_1(0) \in \bar{\mathcal{L}}_k$ are strict invariants of lifts $h(p)$.

Recall that for $m \geqslant 0$,

$$B_m = \sum_{0 \leqslant v \leqslant k \leqslant m} (-1)^v \binom{k}{v} \frac{v^m}{k+1}$$

are the Bernoulli numbers. One of their well-known properties is that

$$x/(1-\exp(-x)) = \sum_{m \geqslant 0} B_m (-x)^m / m! \, .$$

**Proposition 3.8.** *$d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f} = \bar{f}_1 \otimes U$, where*

$$\bar{f}_1 = (\mathrm{ad}\, h(p) \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f} + \sum_{n \geqslant 0} (-1)^n (B_n/n!)[\dots[\bar{c}_1, \underbrace{\bar{f}], \dots, \bar{f}}_{n \ \textit{times}}] \, .$$

*Proof.* In earlier notation we have modulo $U^2$ (use (3.5) and (3.6)):

$$\begin{aligned} \left(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U\right) \bar{f} &\equiv \bar{f} + \bar{f}_1 U \equiv (\bar{c}_1 U) \circ (\bar{f} + \bar{f}^{(1)} U) \\ &\equiv (\bar{f} + \bar{f}^{(1)} U) \circ (U \widetilde{\exp}(\mathrm{ad}\, \bar{f}) \bar{c}_1) \\ &\equiv \bar{f} \circ (E_0(\mathrm{ad}\, \bar{f}) \bar{f}^{(1)} U + \widetilde{\exp}(\mathrm{ad}\, \bar{f}) \bar{c}_1 U) \\ &\equiv \bar{f} + (\bar{f}^{(1)} + E_0(\mathrm{ad}\, \bar{f})^{-1} (\widetilde{\exp}(\mathrm{ad}\, \bar{f})) \bar{c}_1) U \, . \end{aligned}$$

It remains to note that $E_0(x)^{-1} \exp(x) = x/(1-\exp(-x))$. □

**Remark.** a) As we already mentioned the above proposition implies that the knowledge of the differential $\bar{c}_1$ is sufficient to recover the element $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f} = \bar{c}(U) \circ \bar{f}(U)$ and therefore, the element $\bar{c}$. This fact can be obtained directly from the cocycle relation for $\bar{c}(U)$.

b) Suppose $\mathcal{L}'$ is an ideal of $\mathcal{L}$ such that $\mathcal{L}' \supset \mathcal{L}(p)$. Then we can repeat the above arguments to prove that the solutions of (3.4) modulo $\mathcal{L}'_{\mathcal{K}}$ describe uniquely the lifts of $h$ to automorphisms of $\mathcal{K}_{<p}^{G(\mathcal{L}')}$.

3.6. **Special cases.** Recurrent relation (3.4) describes explicitly step by step the action of the lift $h(p)$. We can agree, for example, to find at each step the appropriate values of $\bar{c}_1$ and $V_{a0}$ by the use of the operators $\mathcal{R}$ and $\mathcal{S}$ from Subsection 2.2. This will specify uniquely the lift $h(p)$ together with its action by conjugation on $\bar{\mathcal{L}} = \mathcal{L}/\mathcal{L}(p)$ and, therefore, will determine the structure of $L_h$ (and of the group $\mathcal{G}_h$).

Let (as earlier) $\omega_h^p = \sum_{i \geqslant 0} A_i(h) t^{c_0 + pi}$, where all $A_i(h) \in k$ and $A_0(h) \neq 0$. Then (3.4) modulo $C_2(\bar{\mathcal{L}})_{\mathcal{K}} + \mathcal{M}(p-1)$ gives the following congruence

$$\sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_{a0} \equiv - \sum_{\substack{a \in \mathbb{Z}^0(p) \\ i \geqslant 0}} A_i(h) t^{c_0 + pi - a} a D_{a0} \, . \tag{3.7}$$

Applying the operator $\mathcal{R}$, cf. Lemma 2.2, we obtain:

- $V_{00} = (\mathrm{ad}\, h(p)) D_{00} = \alpha_0 \mathrm{ad}\, h(p) D_0 \in \alpha_0 C_2(\bar{\mathcal{L}})$;

• for all $b \in \mathbb{Z}^+(p)$,

$$V_{b0} = (\operatorname{ad} h(p))D_{b0} \equiv -\sum_{i\geqslant 0} A_i(h)bD_{b+c_0+pi,0} \bmod C_2(\bar{\mathcal{L}})_k\,.$$

The second relation means that all generators of $\bar{\mathcal{L}}_k$ of the form $D_{an}$ with $a > c_0$ can be eliminated from the minimal system of generators of $L_{hk}$. Indeed, because $A_0(h) \neq 0$, all $D_{b+c_0,0}$ belong to the ideal of second commutators $C_2(L_h)_k = ((\operatorname{ad} h(p))\mathcal{L}_k + C_2(\mathcal{L}_k))/\mathcal{L}(p)_k$, and for any $n \in \mathbb{Z}/N_0$, all $D_{b+c_0,n} = \sigma^n D_{b+c_0,0}$ also belong to $C_2(L_h)_k$. The first relation then means that $L_h$ has only one relation with respect to any minimal set of generators. This terminology formally makes sense because in the category of Lie $\mathbb{F}_p$-algebras of nilpotent class $< p$ the algebras of the form $\mathfrak{L}/C_p(\mathfrak{L})$, where $\mathfrak{L}$ is a free Lie $\mathbb{F}_p$-algebra, play a role of free objects. The same remark also can be used for the category of, say, $p$-groups of period $p$ and of nilpotent class $< p$. Therefore, $\mathcal{G}_h$ can be treated as an object of this category with finitely many generators and one relation.

As an illustration of Proposition 3.7, use the relation (3.7) modulo $\mathcal{L}(2)_{\mathcal{K}}+\mathcal{M}(p-1)$ and make the next central step to obtain the following explicit formulas for $V_{a0}$ modulo $\mathcal{L}(3)_k = C_3(L_h)_k$ (the elements $\mathcal{F}^0_{\gamma,-N}$ are generators of ramification ideals introduced in Subsection 1.4).

**Proposition 3.9.** *We have the following congruences modulo* $\mathcal{L}(3)_k$*:*

$$V_{00} \equiv -\alpha_0 \sum_{\substack{i\geqslant 0\\ 0\leqslant n<N_0}} \sigma^n(A_i(h))\sigma^n(\mathcal{F}^0_{c_0+pi,0})\,,$$

*and for all* $a \in \mathbb{Z}^+(p)$*,*

$$V_{a0} \equiv -\sum_{\substack{n\geqslant 1\\ i\geqslant 0}} \sigma^n(A_i(h)\mathcal{F}^0_{c_0+pi+a/p^n,-n}) - \sum_{\substack{m\geqslant 0\\ i\geqslant 0}} \sigma^{-m}(A_i(h)\mathcal{F}^0_{c_0+pi+ap^m,0})\,.$$

Before sketching the proof of this proposition we explain why the sums in the last formula are finite.

**Proposition 3.10.** *Suppose* $a \in \mathbb{Z}^0(p)$*. Then:*

a) *for any* $N, m \geqslant 0$, $\mathcal{F}^0_{c_0+pi+ap^m,-N} \equiv \mathcal{F}^0_{c_0+pi+ap^m,0} \bmod \mathcal{L}(3)_k$*;*

b) *for any* $N \geqslant n \geqslant 1$, $\mathcal{F}^0_{c_0+pi+a/p^n,-N} \equiv \mathcal{F}^0_{c_0+pi+a/p^n,-n} \bmod \mathcal{L}(3)_k$*;*

c) *if* $m \geqslant 0$ *and* $c_0 + pi + ap^m > 2c_0 - 1$ *then* $\mathcal{F}^0_{c_0+pi+ap^m,0} \in \mathcal{L}(3)_k$*;*

d) *if* $n \in \mathbb{N}$ *and* $(c_0 - 1)(1 + p^{-n}) < c_0$ *then* $\mathcal{F}^0_{c_0+pi+a/p^n,-n} \in \mathcal{L}(3)_k$*.*

*Proof.* a) If it is false then $\mathcal{F}^0_{c_0+pi+ap^m,-N}$ should contain a term of the form $a_1[D_{a_10}, D_{a_2n_2}]$, where $n_2 \leqslant -1$ and $a_1 + a_2p^{n_2} = c_0 + pi + ap^m \in \mathbb{Z}$; this implies $a_2 = 0$ and $a_1 = c_0 + pi + ap^m \geqslant c_0$; therefore, $D_{a_10} \in \mathcal{L}(2)_k$ and our commutator belongs to $\mathcal{L}(3)_k$.

b) It is obvious if $a \neq 0$ – in this case both elements don't contain linear terms and for any second commutator $a_1[D_{a_1 0}, D_{a_2 n_2}]$ we should have $a_2 \neq 0$ and $n_2 = -n$. If $a = 0$ then cf. a).

c) $\mathcal{F}^0_{c_0+pi+ap^m,0}$ can contain a linear term only if $m = 0$ which then must be equal to $aD_{c_0+pi+a,0}$, but then $c_0 + pi + a > 2c_0$ and it belongs to $\mathcal{L}(3)_k$; if we have a second commutator $a_1[D_{a_1 0}, D_{a_2 n_2}]$ then the condition $a_1 + p^{n_2} a_2 > 2c_0 - 1$ implies also that this commutator belongs to $\mathcal{L}(3)_k$.

d) In this case there is no linear term, and any appeared second commutator $a_1[D_{a_1 0}, D_{a_2 n_2}]$ should be such that $n_2 = -n$, $a_1, a_2 \leqslant c_0 - 1$ but then $a_1 + a_2 p^{n_2}$ will be less than $c_0 < c_0 + pi + a/p^n$. □

*Proof of Proposition 3.9.* From (3.7) we obtain (apply the operator $\mathcal{S}$ from Subsection 2.2)

$$c_1 \equiv \sum_{\substack{0<a<c_0+pi \\ i,n\geqslant 0}} \sigma^n A_i(h) t^{p^n(c_0+pi-a)} a D_{an} \bmod \mathcal{L}(2)_{\mathcal{K}} + \mathcal{M}(p-1).$$

(Modulo $\mathcal{L}(2)_{\mathcal{K}}$ we can ignore all terms with $a > c_0$.) Then the right-hand side of (3.4) modulo $\mathcal{L}(3)_{\mathcal{K}} + \mathcal{M}(p-1)$ appears as

$$\begin{aligned} -\sum_{a,i} A_i(h) t^{c_0+pi-a} a D_{a0} - \frac{1}{2} \sum_{a_1,a_2,i} A_i(h) t^{c_0+pi-a_1-a_2} a_1 [D_{a_1 0}, D_{a_2 0}] \\ + \frac{1}{2} \sum_{a_1,a_2,i} A_i(h) t^{-(a_1+a_2)} a_1 [D_{a_1+c_0+pi,0}, D_{a_2 0}] \\ - \sum_{\substack{a_1,a_2,n,i \\ 0<a_1<c_0+pi}} \sigma^n(A_i(h)) t^{p^n(c_0+pi-a_1)-a_2} a_1 [D_{a_1,n}, D_{a_2 0}] \end{aligned}$$

In the above sums the indices $a, a_1, a_2$ run over $\mathbb{Z}^0(p)$, $i \geqslant 0$ and $n \geqslant 1$. The third sum can be ignored because all $D_{a_1+c_0+pi,0} \in C_2(L_h)_k$ and for the similar reason we can ignore the restriction $0 < a_1 < c_0 + pi$ in the last sum.

Now note that the terms from the first line can be grouped as follows:

— the constant terms (i.e. the coefficients for $t^0 = 1$) appear as

$$-\frac{1}{2} \sum_i A_i(h) \sum_{a_1+a_2=c_0+pi} a_1 [D_{a_1 0}, D_{a_2 0}] = -\sum_i A_i(h) \mathcal{F}^0_{c_0+pi,0};$$

— the remaining terms are grouped with respect to the condition $a = c_0 + pi + b$ or $a_1 + a_2 = c_0 + pi + bp^m$, where $b \in \mathbb{Z}^+(p)$ and $m \geqslant 0$, and appear as

$$-\sum_i A_i(h) \sum_{b,m} t^{-bp^m} \mathcal{F}^0_{c_0+pi+bp^m,0};$$

The terms from the last line are grouped (modulo $\mathcal{L}(3)_{\mathcal{K}}$) with respect to the condition $a_1 + a_2/p^n = c_0 + pi + b/p^n$, where $b \in \mathbb{Z}^+(p)$ and $n \geqslant 1$, and appear as

$$-\sum_i \sigma^n(A_i(h)) \sum_a t^{-a} \sigma^n \mathcal{F}^0_{c_0+pi+a/p^n,-n}\,.$$

It remains to recover the values of $V_b$ by applying the operator $\mathcal{R}$ from Subsection 2.2. □

## 4. Application 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 $\pi_0$ be a uniformising element in $K$. Denote by $\bar{K}$ an algebraic closure of $K$, set $\Gamma = \mathrm{Gal}(\bar{K}/K)$. We assume that $K$ contains a primitive $p$-th root of unity $\zeta_1$.

Let $\Gamma_{<p} := \Gamma/\Gamma^p C_p(\Gamma)$. We are going to apply the above results for the group $\mathcal{G}_h$ to the group $\Gamma_{<p}$. Our exposition is not very far from Section 4 of [7], but we do not discuss the structure of ramification filtration, simplify constructions and correct some inexactitudes.

4.1. **Exact sequences for $\Gamma_{<p}$.** For $n \in \mathbb{N}$, choose $\pi_n \in \bar{K}$ such that $\pi_n^p = \pi_{n-1}$. Let $\widetilde{K} = \bigcup_{n\in\mathbb{N}} K(\pi_n)$, and $\Gamma_{\widetilde{K}} = \mathrm{Gal}(\bar{K}/\widetilde{K})$. Then the embedding $\Gamma_{\widetilde{K}} \subset \Gamma$ induces $\iota : \Gamma_{\widetilde{K}} \longrightarrow \Gamma_{<p}$. Note that $\mathrm{Gal}(K(\pi_1)/K) = \langle\tau_0\rangle^{\mathbb{Z}/p}$, where $\tau_0(\pi_1) = \pi_1\zeta_1$.

Let $j : \Gamma_{<p} \longrightarrow \mathrm{Gal}(K(\pi_1)/K)$ be a natural epimorphism. The following proposition appears as Proposition 4.1 from [7] when $M = 1$.

**Proposition 4.1.** *The following sequence is exact*

$$\Gamma_{\widetilde{K}} \xrightarrow{\iota} \Gamma_{<p} \xrightarrow{j} \langle\tau_0\rangle^{\mathbb{Z}/p} \longrightarrow 1\,.$$

Let $R$ be Fontaine's ring. There is a natural embedding $k \subset R$ and $t = (\pi_n \bmod p)_{n\geqslant 0} \in R$. If $\mathcal{K} = k((t))$ and $R_0 = \mathrm{Frac}\, R$ then $\mathcal{K}$ is a closed subfield of $R_0$ and the field-of-norms functor $X$, cf. [20] Subsection 4.3, identifies $X(\widetilde{K})$ with $\mathcal{K}$ and $R_0$ with the completion of $\mathcal{K}_{sep}$. In particular, there is a natural inclusion $\iota_K : \Gamma \longrightarrow \mathrm{Aut}\, R_0$ which induces the identification of $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$ and $\Gamma_{\widetilde{K}}$.

We use the results of the above sections and the appropriate notation related to our field $\mathcal{K}$, e.g. $\mathcal{G}_{<p} = \mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K})$, where $\mathcal{K}_{<p} = \mathcal{K}_{sep}^{\mathcal{G}^p C_p(\mathcal{G})}$. The identification $\iota_K|_{\Gamma_{\widetilde{K}}}$ composed with the morphism $\iota$ from Proposition 4.1 induces a group homomorphism $\iota_{<p} : \mathcal{G}_{<p} \longrightarrow \Gamma_{<p}$ and Proposition 4.1 implies the following property.

**Proposition 4.2.** *The following sequence is exact*

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

4.2. **Auxiliary statements.** Let $v_{\mathcal{K}}$ be a unique extension of the normalized valuation of $\mathcal{K}$ to $R_0$. Let $\eta$ be a closed embedding of $\mathcal{K}$ into $R_0$ which is compatible with $v_{\mathcal{K}}$, i.e. for any $a \in \mathcal{K}$, $v_{\mathcal{K}}(a) = v_{\mathcal{K}}(\eta(a))$.

Let $c_0 := e^*(= e_K p/(p-1))$. As earlier, consider the embeddings $\mathcal{M} \subset \mathcal{L}_{\mathcal{K}}$, $\mathcal{M}_{<p} \subset \mathcal{L}_{\mathcal{K}_{<p}}$ and their analogue

$$\mathcal{M}_{R_0} = \sum_{1 \leqslant s < p} t^{-sc_0} \mathcal{L}(s_0)_{\mathrm{m}_R} + \mathcal{L}(p)_{R_0} \subset \mathcal{L}_{R_0}\,,$$

where $\mathrm{m}_R$ is the maximal ideal in $R$.

We know that $e \in \mathcal{M}$, $f \in \mathcal{M}_{<p}$ (these elements were chosen in Subsection 1.3) and for similar reasons, if $\hat{\eta} \in \mathrm{Aut}R_0$ is a lift of $\eta$ then $(\mathrm{id}_{\mathcal{L}} \otimes \hat{\eta})f \in \mathcal{M}_{R_0}$.

Below we consider the condition $(\mathrm{id}_{\mathcal{L}} \otimes \eta)e \equiv e \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$. In particular, this congruence holds modulo $\mathcal{L}_{\mathrm{m}_R} + \mathcal{L}(p)_{R_0}$ and following the coefficient for $D_{10}$ we deduce that $\eta|_k = \mathrm{id}$.

**Proposition 4.3.** *Suppose* $(\mathrm{id}_{\mathcal{L}} \otimes \eta)e \equiv e \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$. *Then*

a) *there is* $m \in t^{(p-1)c_0}\mathcal{M}_{R_0}$ *such that*

$$(\mathrm{id}_{\mathcal{L}} \otimes \eta)e \equiv (-\sigma m) \circ e \circ m \bmod \mathcal{L}(p)_{R_0}\,;$$

b) *if* $\hat{\eta}$ *is a lift of* $\eta$ *to* $R_0$ *then there is a unique* $l \in G(\mathcal{L}) \bmod G(\mathcal{L}(p))$ *such that*

$$(\mathrm{id}_{\mathcal{L}} \otimes \hat{\eta})f \equiv f \circ l \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}\,;$$

c) *there is a unique lift* $\eta(p)$ *of* $\eta$ *to* $\mathcal{K}(p)$ *such that* $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta(p))\bar{f} = \bar{f}$, *where* $\bar{f} = f \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$.

*Proof.* a) Note that $t^{(p-1)c_0}\mathcal{M}_{R_0}$ is an ideal in $\mathcal{M}_{R_0}$ and for any $i \in \mathbb{N}$ and $m^0 \in t^{(p-1)c_0}C_i(\mathcal{M}_{R_0})$, there is $m_i \in t^{(p-1)c_0}C_i(\mathcal{M}_{R_0})$ such that $\sigma m_i - m_i \equiv m^0 \bmod \mathcal{L}(p)_{R_0}$. (Use that $\sigma$ is topologically nilpotent on $t^{(p-1)c_0}\mathcal{M}_{R_0}/\mathcal{L}(p)_{R_0}$.)

Therefore, there is $m_1 \in t^{(p-1)c_0}\mathcal{M}_{R_0}$ such that $\eta(e) \equiv e - \sigma m_1 + m_1 \bmod \mathcal{L}(p)_{R_0}$. This implies that

$$\sigma(m_1) \circ \eta(e) \equiv e \circ m_1 \bmod t^{(p-1)c_0}C_2(\mathcal{M}_{R_0}) + \mathcal{L}(p)_{R_0}\,.$$

Similarly, there is $m_2 \in t^{(p-1)c_0}C_2(\mathcal{M}_{R_0})$ such that

$$\sigma(m_1) \circ \eta(e) \equiv -\sigma m_2 + m_2 + e \circ m_1 \bmod \mathcal{L}(p)_{R_0},$$

$$\sigma(m_2 \circ m_1) \circ \eta(e) \equiv e \circ (m_2 \circ m_1) \bmod t^{(p-1)c_0}C_3(\mathcal{M}_{R_0}) + \mathcal{L}(p)_{R_0}\,,$$

and so on. This gives $m_i \in t^{(p-1)c_0}C_i(\mathcal{M}_{R_0})$, $1 \leqslant i < p$, such that

$$\sigma(m_{p-1} \circ \cdots \circ m_1) \circ \eta(e) \equiv e \circ (m_{p-1} \circ \cdots \circ m_1) \bmod \mathcal{L}(p)_{R_0}\,.$$

This proves a) with $m = m_{p-1} \circ \cdots \circ m_1$.

b) Let $(\mathrm{id}_{\mathcal{L}} \otimes \hat{\eta})f = f'$. Then for the above element $m$, we have $\sigma(m \circ f') \equiv e \circ (m \circ f') \bmod \mathcal{L}(p)_{R_0}$ and, therefore,

$$\sigma((-f) \circ m \circ f') \equiv (-f) \circ m \circ f' \bmod \mathcal{L}(p)_{R_0}\,.$$

This implies the existence of $l \in \mathcal{L}$ such that $m \circ f' \equiv f \circ l \bmod \mathcal{L}(p)_{R_0}$ (use that $\bar{\mathcal{L}}_{R_0}|_{\sigma=\mathrm{id}} = \bar{\mathcal{L}}$).

Suppose $l' \in \mathcal{L}$ also satisfies statement b) of our lemma. Then we have $f \circ l \equiv f \circ l' \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$, $l \equiv l' \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$ and

$$l \circ (-l') \in \left(t^{(p-1)c_0}\mathcal{M}_{R_0}\right)|_{\sigma=\mathrm{id}} \subset (\mathcal{L}_{\mathrm{m}_R} + \mathcal{L}(p)_{R_0})|_{\sigma=\mathrm{id}} = \mathcal{L}(p)\,.$$

c) This follows from part b) because $\mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K}(p)) = \mathcal{L}(p)$.

Proposition is proved. □

4.3. **Isomorphism $\kappa_{<p}$.** Let $\varepsilon = (\zeta_n \bmod p)_{n\geqslant 0} \in R$ be Fontaine's element (here $\zeta_1 \in K$ is our $p$-th root of unity and for all $n$, $\zeta_n^p = \zeta_{n-1}$).

Let $\zeta_1 = 1 + \pi_0^{c_0/p}\sum_{i\geqslant 0}[\beta_i]\pi_0^i$, where all $[\beta_i]$ are the Teichmuller representatives of $\beta_i \in k$. Use the identification of rings $R/t^{pe_K} \simeq O_{\bar{K}}/p$, coming from the projection $R \longrightarrow (O_{\bar{K}}/p)_1$. This implies

$$\varepsilon \equiv 1 + \sum_{i\geqslant 0}\alpha_i t^{c_0+pi} \bmod t^{(p-1)c_0}R$$

where all $\alpha_i = \beta_i^p \in k$, $\alpha_0 \neq 0$ (note that $pe_K = (p-1)c_0$ and $\varepsilon \notin \mathcal{K}$).

Assume that $h \in \mathrm{Aut}\mathcal{K}$ from Subsection 2.1 is such that for all $i$, $\alpha_i(h) = \alpha_i$ (and $h|_k = \mathrm{id}_k$). Then

$$h(t) \equiv t\varepsilon \bmod t^{(p-1)c_0+1}R\,.$$

This implies that for any $\tau \in \Gamma$, there is $\tilde{h} \in \langle h\rangle \subset \mathrm{Aut}\,\mathcal{K}$ such that $\iota_K(\tau)|_{\mathcal{K}}(t) \equiv \tilde{h}(t) \bmod t^{(p-1)c_0+1}R$. Indeed, there is $m \in \mathbb{Z}_p$ such that

$$\iota_K(\tau)(t) = t\varepsilon^m \equiv t\left(1 + \sum_{i\geqslant 0}\alpha_i t^{c_0+pi}\right)^m \equiv h^m(t) \bmod t^{(p-1)c_0+1}R$$

(use that $h(t^p) \equiv t^p \bmod t^{pc_0}R$), and we can take $\tilde{h} = h^m$. Clearly, such $\tilde{h}$ is unique modulo the subgroup $\langle h^p\rangle$.

This means that $\eta := \iota_K(\tau)|_{\mathcal{K}}\tilde{h}^{-1} : \mathcal{K} \longrightarrow R_0$ satisfies the assumption from Proposition 4.3. Let $\eta(p)$ be the lift from part c) of that proposition, let $\hat{\eta} \in \mathrm{Aut}R_0$ be such that $\hat{\eta}|_{\mathcal{K}(p)} = \eta(p)$ and set $\tilde{h}(p) := (\hat{\eta}^{-1}\iota_K(\tau))|_{\mathcal{K}(p)}$. Then $\tilde{h}(p)|_{\mathcal{K}} = \tilde{h}$ and by Galois theory $\tilde{h}(p) \in \mathrm{Aut}\,\mathcal{K}(p)$. As a result, $\tilde{h}(p) \in \widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h)$ is a unique lift of $\tilde{h}$ such that

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \tilde{h}(p))\bar{f}\,.$$

If $\tilde{h}$ is multiplied by an element of $\langle h^p\rangle$ then $\tilde{h}(p)$ is multiplied by an element from $(\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h))^p$ but this will not affect $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \tilde{h}(p))\bar{f}$. Therefore, the image of $\tilde{h}(p)$ in $\mathcal{G}_h$ is well-defined. We obtained the map of sets $\kappa : \Gamma \longrightarrow \mathcal{G}_h$ uniquely characterized by the equality

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau))\bar{f}\,,$$

where $\hat{\kappa}(\tau) \in \widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h) \subset \mathrm{Aut}\mathcal{K}(p)$ is any lift of $\kappa(\tau) \in \mathcal{G}_h$ with respect to the natural projection $\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h) \longrightarrow \mathcal{G}_h$.

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

*Proof.* Suppose $\tau_1, \tau \in \Gamma_K$. Let $\bar{c} \in \bar{\mathcal{L}}_{\mathcal{K}}$ and $\bar{A} \in \mathrm{Aut}_{\bar{\mathcal{L}}}$ be such that $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau))\bar{f} = \bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}$. Then

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1))(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau))\bar{f}$$

$$= (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1))(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1))(\bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}) =$$

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1))\bar{c} \circ (\bar{A} \otimes \iota_K(\tau_1))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1))\bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\tau_1))\bar{f}$$

$$= (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1))\bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1))(\bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}$$

$$= (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1))(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau))\bar{f} = (\mathrm{id}_{\bar{\mathcal{L}}} \otimes \hat{\kappa}(\tau_1)\hat{\kappa}(\tau))\bar{f}$$

and, therefore, $\kappa(\tau_1\tau) = \kappa(\tau_1)\kappa(\tau)$ (use that $\mathcal{G}_h$ acts strictly on the orbit of $\bar{f}$). In particular, $\kappa$ 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 of $\Gamma_{\widetilde{K}}$ with $\mathcal{G}$ and, therefore, $\kappa_{<p}$ identifies the groups $\kappa(\Gamma_{\widetilde{K}})$ and $G(\bar{\mathcal{L}}) \subset \mathcal{G}_h$. Besides, $\kappa_{<p}$ induces a group isomorphism of $\langle\tau_0\rangle^{\mathbb{Z}/p}$ and $\langle h\rangle^{\mathbb{Z}/p}$. Now Proposition 4.2 implies that $\kappa_{<p}$ is a group isomorphism. □

4.4. **Properties of $\Gamma_{<p} = G(L)$.** By Proposition 4.4 the results obtained for the group $\mathcal{G}_h$ in the characteristic $p$ case can be extended to the Galois group $\Gamma_{<p}$ coming from the mixed characteristic case. These results were stated independently in the Introduction. We summarize them here briefly as follows:

— $\Gamma_{<p} = G(L)$, where $L$ is the Lie $\mathbb{F}_p$-algebra such that

$$0 \longrightarrow \mathcal{L}/\mathcal{L}(p) \longrightarrow L \longrightarrow \mathbb{F}_p\tau_0 \longrightarrow 0\,;$$

— the Lie algebra $\mathcal{L}$ was defined in Subsection 1.3;

— $\mathcal{L}_k$ has system of generators $\{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{D_0\}$;

— the ideals $\mathcal{L}(s)$, $2 \leqslant s \leqslant p$, are given by Theorem 2.5 and the ideal $C_s(L)$ of commutators of order $\geqslant s$ in $L$ equals $\mathcal{L}(s)/\mathcal{L}(p)$;

— the structure of $L$ is determined by a lift $\tau_{<p}$ of $\tau_0$ and the appropriate differentiation $\mathrm{ad}\tau_{<p}$ is described via recurrent relation (3.4).

## References


[1] V.A.Abrashkin, *Ramification filtration of the Galois group of a local field*, Proceedings of the St. Petersburg Mathematical Society III, Amer. Math. Soc. Transl. Ser. 2, (1995) **166**, Amer. Math. Soc., Providence, RI

[2] V.A. Abrashkin, *Ramification filtration of the Galois group of a local field. II*, Proceedings of Steklov Math. Inst. **208** (1995)

[3] V.Abrashkin, *Ramification filtration of the Galois group of a local field. III*, Izvestiya RAN: Ser. Mat., **62**, no.5 (1998), 3-48; English transl. Izvestiya: Mathematics **62**, no.5, 857–900

[4] V. Abrashkin, *On a local analogue of the Grothendieck Conjecture*, Int. J. Math. (2000) **11**, no.1, 3–43

[5] V. Abrashkin, *Modified proof of a local analogue of the Grothendieck Conjecture*, Journal Théorie des Nombres de Bordeaux **22**, (2010), 1-50

[6] V.Abrashkin, *Galois groups of local fields, Lie algebras and ramification.* In: Arithmetic and Geometry, eds. Dieulefait, L., Faltings, G., Heath-Brown, D.R., Manin, Yu., Moroz, B.Z., Wintenberger, J.-P. Cambridge University Press. **420**: 1-23

[7] V. Abrashkin, *Groups of automorphisms of local fields of period $p^M$ and nilpotent class $< p$*, to appear in Ann. Inst. Fourier

[8] V. Abrashkin, *Groups of automorphisms of local fields of period p and nilpotent class $< p$, II.*

[9] N. Bourbaki, *Elements of Mathematics. Lie Groups and Lie Algebras.*

[10] M. Hall The theory of groups, The Macmillan Company New York, 1959

[11] U. Jannsen, K. Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper*, Invent. math. (1982) **70**, 71-98

[12] H.Koch, Galois theory of $p$-extensions, Springer Monographs in Mathematics, 2002, XIII, 191 p

[13] F. Laubie *Extensions de Lie et groupes d'automorphismes de corps locaux*, Comp. Math., **67** (1988), 165-189

[14] F.Laubie *Une théorie du corps de classes local non abélien*, Compos. Math., **143** (2007), no. 2, 339–362.

[15] M. Lazard, *Sur les groupes nilpotentes et les anneaux de Lie*, Ann. Ecole Norm. Sup. (1954) **71**, 101-190

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

[17] J.-P.Serre, *Local Fields*. Berlin, New York: Springer-Verlag, 1980

[18] J.-P.Serre, Cohomologie Galoisienne Springer Verlag, Berlin-Gottingen-Heidelberg-New York, 1964

[19] J.-P.Serre Bourbaki *Structure de certains pro-p-groupes (d'aprés Demushkin)*. Séminaire Bourbaki, **8**, Exp. No. 252, 145155, Soc. Math. France, Paris, 1995.

[20] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies des corps locaux; application.* Ann. Sci. Ec. Norm. Super., IV. Ser, **16** (1983), 59–89

[21] W. Zink *Ramification in local Galois groups; the second central step*, Pure Appl. Math. Q. **5** (2009), no. 1, 295–338.



Department of Mathematical Sciences, Durham University, Science Laboratories, South Rd, Durham DH1 3LE, United Kingdom & Steklov Institute, Gubkina str. 8, 119991, Moscow, Russia

*E-mail address*: victor.abrashkin@durham.ac.uk