AUTOMORPHISMS OF LOCAL FIELDS OF PERIOD \( p \) AND NILPOTENT CLASS \(< p \)

VICTOR ABRASHKIN

Abstract. Suppose \( K \) is a finite field extension of \( \mathbb{Q}_p \) containing a primitive \( p \)-th root of unity. Let \( \Gamma_K(1) \) be the Galois group of a maximal \( p \)-extension of \( K \) with the Galois group of period \( p \) and nilpotent class \(< p \). In the paper we describe the ramification filtration \( \{\Gamma_K(1)^{(v)}\}_{v \geq 0} \) and relate it to an explicit form of the Demushkin relation for \( \Gamma_K(1) \). The results are given in terms of Lie algebras attached to involved groups by the classical equivalence of the categories of \( p \)-groups and Lie algebras of nilpotent class \(< p \).

Introduction

Everywhere in the paper \( p \) is a prime number, \( p > 2 \).

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 \( \geq s \). With this notation, \( G/G^pC_s(G) \) 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 \( s \) and \( L/C_s(L) \) is the maximal quotient of nilpotent class \(< s \) of \( L \). For any topological \( \mathbb{F}_p \)-module \( \mathcal{M} \) we use the notation \( L\mathcal{M} = L \otimes_{\mathbb{F}_p} \mathcal{M} \).

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

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

has \( p \)-integral coefficients modulo \( p \)-th commutators. Therefore, for any topological Lie \( \mathbb{F}_p \)-algebra \( L \) of nilpotent class \(< p \), we can introduce the topological group \( G(L) \) which equals \( L \) as a set and is provided with the Campbell-Hausdorff composition law \( l_1 \circ l_2 = l_1 + l_2 + (1/2)[l_1, l_2] + \ldots \). The correspondence \( L \mapsto G(L) \) induces equivalence of the category of Lie \( \mathbb{F}_p \)-algebras of nilpotent class \(< p \) and the category of \( p \)-groups of period \( p \) of the same nilpotent class.

Let \( K \) be a complete discrete valuation field with finite residue field \( k \cong \mathbb{F}_p^{\times_0} \), \( N_0 \in \mathbb{N} \). Denote by \( K_{\text{sep}} \) a separable closure of \( K \) and set \( \text{Gal}(K_{\text{sep}}/K) = \Gamma_K \).

A profinite group structure of \( \Gamma_K \) is well-known, \([18]\). Most significant information about this structure comes from the maximal \( p \)-quotient \( \Gamma_K(p) \) of \( \Gamma_K \), \([19, 26, 27]\). As a matter of fact, the structure

\[\text{Date: March 16, 2014.}\]

\[\text{Key words and phrases.} \ \text{local field, Galois group, ramification filtration.}\]
of $\Gamma_K(p)$ 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 $\text{char} K = p$) then $\Gamma_K(p)$ is pro-finite free; otherwise, $\Gamma_K(p)$ has only one (the Demushkin) relation of a very special form.

On the other hand, $\Gamma_K$ has additional structure given by decreasing series of normal (ramification) subgroups $\Gamma_K^{(v)}$, $v \geq 0$. This additional structure on $\Gamma_K$ (or even on the pro-$p$-group $\Gamma_K(p)$) is sufficient to recover all properties of the original complete discrete valuation field $K$, $[24,6,10]$. Note that on the level of abelian extensions the ramification filtration of $\Gamma_K^{ab}$ is completely described by class field theory and has very simple structure. But already on the level of $p$-extensions with Galois groups of nilpotent class $\geq 2$, the ramification filtration starts demonstrating highly non-trivial behaviour, cf. $[2,4,15,16]$.

In $[1,2,3]$ the author introduced new techniques (nilpotent Artin-Schreier theory) which allowed us to work with field extensions of characteristic $p$ with Galois groups of nilpotent class $< p$. As we have mentioned already, such groups come from Lie algebras and our main result describes the ideals coming from ramification subgroups.

Consider the case of complete discrete valuation fields $K$ of mixed characteristic containing a primitive $p$-th root of unity $\zeta_1$. Let $K_{<p}$ be the maximal $p$-extension of $K$ in $K_{\text{sep}}$ with the Galois group of nilpotent class $< p$ and period $p$. Then $\text{Gal}(K_{<p}/K) = \Gamma_K/\Gamma_K^{p}C_p(\Gamma_K) := \Gamma_K(1)$ is a group with finitely many generators and one relation. (This terminology makes sense in the category of $p$-groups of nilpotent class $< p$ and period $p$.) Let $\{\Gamma_K(1)^{(v)}\}_{v \geq 0}$ be the ramification filtration of $\Gamma_K(1)$. If $L$ is a Lie $\mathbb{F}_p$-algebra such that $\Gamma_K(1) = G(L)$ then for all $v$, $\Gamma_K(1)^{(v)} = G(L^{(v)})$, where $L^{(v)}$ are ideals in $L$. In this paper we determine the structure of $L$ and “ramification” ideals $L^{(v)}$. In particular, the Demushkin relation in $L$ appears in our setting in terms related directly to ramification ideals $L^{(v)}$.

Note that a similar technique (the paper in progress) can be used to treat not only more general groups $\Gamma_K(M) := \Gamma_K/\Gamma_K^{pM}C_p(\Gamma_K)$, $M \in \mathbb{N}$, but also the case of higher local fields $K$.

For the first approach to the above problem cf. $[31]$, where the image of the ramification filtration in $C_2(\Gamma_K)/\Gamma_K^{p}C_3(\Gamma_K)$ was studied under some restrictions to the basic field $K$. The methods and techniques from $[31]$ could not be applied to more general situation.

The principal advantage of our method is that from the very beginning we work with the whole group $\Gamma_K(1)$ rather than with the appropriate sequence of central extensions.

The main steps of our approach can be described as follows.

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 $\pi_p^n = \pi_{n-1}$. Then the field-of-norms functor $X$, gives us a complete discrete valuation field $X(\widetilde{K}) = K$ of characteristic $p$ with residue field $k$ and fixed uniformizer $t$. We have also a natural identification $\Gamma_K = \Gamma_{\widetilde{K}}$, which is compatible with the appropriate ramification filtrations in $\Gamma_K$ and $\Gamma_{\widetilde{K}}$ via the Herbrand function $\varphi_{\widetilde{K}/K}$. This gives us the following fundamental short exact sequence in the category of $p$-groups
\begin{equation}
\Gamma_K(1) \xrightarrow{\iota} \Gamma_K(1) \longrightarrow \text{Gal}(K(\pi)/K) \left( = \langle \tau \rangle \mathbb{Z}/p \right) \longrightarrow 1,
\end{equation}
where $\tau_0$ is such that $\tau_0(\pi) = \zeta \pi$.

b) Nilpotent Artin-Schreier theory.

This theory allows us to fix an identification $\Gamma_K(1) = G(L)$, where $L$ is profinite Lie algebra over $\mathbb{F}_p$. This identification depends only on the above uniformizer $t$ in $K$ and a choice of $\alpha_0 \in k$ such that $T_{k/\mathbb{F}_p}(\alpha_0) = 1$. Note that we also are provided with a system of free generators $\{D_{an} \mid (a, p) = 1, n \in \mathbb{Z}/N_0\} \cup \{D_0\}$ of $L_k$.

c) Ramification filtration in $\Gamma_K(1)$.

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

d) Fundamental sequence of Lie algebras.

Using the above mentioned equivalence of the categories of $p$-groups and Lie algebras we can replace (0.1) by the following exact sequence of Lie $\mathbb{F}_p$-algebras
\begin{equation}
0 \longrightarrow L/L(p) \longrightarrow L \longrightarrow \mathbb{F}_p \tau_0 \longrightarrow 0,
\end{equation}
where $G(L(p)) = \text{Ker } \iota$ and $G(L) = \Gamma_K(1)$. If $\hat{\tau}_0$ is a lift of $\tau_0$ to $L$ then the structure of (0.2) can be given via the differentiation $\text{ad}_{\hat{\tau}_0}$ on $L$.

e) Replacing $\tau_0$ by $h_0 \in \text{Aut} \mathcal{K}$

When studying the structure of (0.2) we can approximate $\tau_0$ by $h_0 \in \text{Aut} \mathcal{K}$. This automorphism $h_0$ is defined in terms of expansion of $\zeta$ as a power series in $\pi_0$. Then the formalism of nilpotent Artin-Schreier theory allows us to specify a lift $\hat{\tau}_0$, to find the ideal $L(p)$ and to introduce a recurrent procedure to obtain the values $\text{ad}_{\hat{\tau}_0}(D_{an}) \in L_k$ and $\text{ad}_{\hat{\tau}_0}(D_0) \in L$.

f) Structure of $L$.

Analyzing the above recurrent procedure modulo $C_2(L_k)$ we can see that the knowledge of $\text{ad}_{\hat{\tau}_0}(D_{an})$ allows us to kill all generators $D_{an}$ of
\[ L_k \] with \( a > c_0 := e_K p/(p-1) \). (Here \( e_K \) is the ramification index of \( K \) over \( \mathbb{Q}_p \).) In other words, \( L_k \) has the minimal system of generators \( \{ D_{an} \mid 1 \leq a < c_0, n \in \mathbb{Z}/N_0 \} \cup \{ D_0 \} \cup \{ \tilde{\tau}_0 \} \). On the other hand, \( \text{ad}\tilde{\tau}_0(D_0) \in C_2(L_k) \) and, therefore, gives us the Demushkin relation in \( L \).

\( g) \) Ramification subgroups \( L^{(v)} \) in \( L \).

For \( v < c_0 \), all ramification ideals \( L^{(v)} \subset L/\mathcal{L}(p) \) and, therefore, appear from the appropriate ideals \( \mathcal{L}^{(v')} \), where the upper indices \( v \) and \( v' \) are related by the Herbrand function of the field extension \( \tilde{K}/K \). It remains only to specify a “good” lift \( \tilde{\tau}_0 \) of \( \tau_0 \), i.e. such that \( \tilde{\tau}_0 \in L^{(c_0)} \). This is most difficult part of the paper where we need a technical result from [3]. As one of applications we found for \( 2 \leq s < p \), the biggest upper ramification numbers of the maximal \( p \)-extensions \( K[s] \) of \( K \) with the Galois groups of period \( p \) and nilpotent class \( \leq s \).

\( h) \) Explicit formulas for \( \text{ad}\tilde{\tau}_0 \) with “good” \( \hat{\tau}_0 \).

The formulas for \( \text{ad}\hat{\tau}_0(D_{am}) \) and \( \text{ad}\hat{\tau}_0(D_0) \) can be easily obtained modulo \( C_3(L_k) \). In Section 5 we obtain a general formula for \( \text{ad}\hat{\tau}_0(D_1) \). This gave an explicit form of the Demushkin relation in terms of ramification generators \( \mathcal{F}_0^{\gamma_1,-N} \).

Note that our description of the Galois group \( \Gamma_K(1) \) together with its ramification filtration may serve as a guide to what we could expect a nilpotent class field theory should be. It would be very interesting to compare our results with the construction of \( \Gamma_K \) in [22], cf. also [20]. This construction uses iterations of Lubin-Tate theories via the field-of-norms functor and is done inside the group of formal power series with operation given by their composition. In the moment, it is not clear how to extract from this construction well-known properties of, say, pro-\( p \)-group \( \Gamma_K(p) \).

The content of this paper is arranged in a slightly different order compared to above principal steps a)-h). In Section 1 we briefly discuss auxiliary facts from the characteristic \( p \) case. In section 2 we study an analogue \( \mathcal{G}_{h_0} \) of \( \Gamma_K(1) \) which appears if we replace \( \tau_0 \) by a suitable \( h_0 \in \text{Aut}K \); we also described the commutator subgroups of \( \mathcal{G}_{h_0} \) and, in particular, found \( \mathcal{L}(p) = C_p(\mathcal{G}_{h_0}) \). In Section 3 we develop the techniques allowing us to switch the languages of \( p \)-groups and Lie algebras. In Section 4 we establish the Criterion to characterize “good” lifts \( \hat{h}_0 \) and in Section 5 we compute \( \text{ad}\hat{h}_0(D_0) \) for such “good” lifts. Finally, in Section 6 we prove that all our results obtained for the group \( \mathcal{G}_{h_0} \) are actually valid for the group \( \Gamma_K(1) \).

1. Preliminaries
1.1. Covariant nilpotent Artin-Schreier theory. Suppose $\mathcal{K}$ is a field of characteristic $p$, $\mathcal{K}_{\text{sep}}$ is a separable closure of $\mathcal{K}$ and $\mathcal{G} = \text{Gal}(\mathcal{K}_{\text{sep}}/\mathcal{K})$. We assume that the composition $g_1g_2$ of $g_1, g_2 \in \mathcal{G}$ is such that for any $a \in \mathcal{K}_{\text{sep}}$, $g_1(g_2a) = (g_1g_2)a$.

In [1] we developed a nilpotent analogue of the classical Artin-Schreier theory of cyclic extensions of fields 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 $g_2g_1$. In other words, we assume that $\mathcal{G}^0$ acts on $\mathcal{K}_{\text{sep}}$ via $(g_1g_2)a = g_2(g_1(a))$.

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

For any $e \in G(L_{\mathcal{K}})$, the set of $f \in G(L_{\mathcal{K}_{\text{sep}}})$ 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 $g \in \mathcal{G}$, $\pi_f^0(e) : g \mapsto g(f) \circ (-f)$.

We have the following properties:

- a) for any group homomorphism $\eta : \mathcal{G}^0 \to G(L)$ there are $e \in G(L_{\mathcal{K}})$ and $f \in G(L_{\mathcal{K}_{\text{sep}}})$ such that $\sigma(f) = f \circ e$ and $\eta = \pi_f^0(e)$;
- b) two homomorphisms $\pi_f^0(e_1)$ and $\pi_{f'}^0(e_1)$ from $\mathcal{G}^0$ to $G(L)$ are conjugated via an 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 $\pi_f(e) : \mathcal{G} \to G(L)$. Then we have the obvious analogs of above properties a) and b) with the opposite formula $e_1 = \sigma(x) \circ e \circ (-x)$ for $e_1$.

In this 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 $\text{Aut}\mathcal{K}$ and $\text{Aut}\mathcal{K}_{\text{sep}}$ be the groups of continuous automorphisms of $\mathcal{K}$ and $\mathcal{K}_{\text{sep}}$, respectively. For $h \in \text{Aut}\mathcal{K}$, let $\hat{h} \in \text{Aut}\mathcal{K}_{\text{sep}}$ be such that $\hat{h}|_{\mathcal{K}} = h$.

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

Proposition 1.1. The following conditions are equivalent:

- a) $\hat{h}(\mathcal{K}_e) = \mathcal{K}_e$;
b) there are \( x \in G(L_K) \) and \( a \in \text{Aut}L \) such that \( \hat{h}(f) = x \circ (a \otimes \text{id})(f) \).

**Proof.** Let \( e_1 = h(e) \), \( f_1 = \hat{h}(f) \) and \( \eta_1 = \pi_{f_1}(e_1) \). Then for any \( g \in G \), we have \( \eta_1(g) = (-f_1) \circ g(f_1) = \hat{h}((-f) \circ (h^{-1}g\hat{h}(f))) = \eta(h^{-1}gh) \). Therefore, \( \eta_1 \) is equal to the composition of the conjugation \( g \mapsto h^{-1}gh \) and \( \eta \). Then \( \hat{h}(K_e) = K_e \) means that \( \text{Ker} \eta = \text{Ker} \eta_1 \). 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 \( f' = (a \otimes \text{id})(f) \) and \( e' = (a \otimes \text{id})e \). Then \( \pi_{f'}(e')(g) = (a \otimes \text{id})((-f) \circ g(f)) = (a \eta)(g) = \eta_1(g) \). This means that \( f' \) and \( f_1 \) give the same morphisms \( L \to G(L) \) and there is an \( x \in G(L_K) \) such that \( f_1 = x \circ f' \), that is \( a \) implies \( b \). Proceeding in the opposite direction we deduce \( b \) from \( a \).

1.3. The identification \( \eta_0 \). Let \( K = k((t)) \) 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 \( T_{k/'\mathbb{F}_p} \alpha_0 = 1 \).

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

Let \( \mathcal{L} = \hat{\mathcal{L}}_k^0/\mathbb{C}_p(\mathcal{L}^0) \).

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

Consider \( e_0 = \sum_{a \in \mathbb{Z}^0(p)} \ell^{-a}D_{an} \in G(\mathcal{L}_K) \). Choose \( f_0 \in G(\mathcal{L}_{K^{sep}}) \) such that \( \sigma(f_0) = e_0 \circ f_0 \). Then the morphism \( \pi_{f_0}(e_0) \) induces the isomorphism of topological groups \( \eta_0 : G_{<p} = : G/\mathbb{C}_p(G) \to G(\mathcal{L}) \).

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

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

\[
\mathcal{F}_{\gamma,-N}^0 = \sum_{1 \leq s < p \atop a_1, \ldots, a_s} a_1 \eta(n_1, \ldots, n_s) [D_{a_1n_1}, D_{a_2n_2}, \ldots, D_{a_sn_s}]
\]

Here:

- all \( a_i \in \mathbb{Z}^0(p), n_i \in \mathbb{Z}, 0 = n_1 \geq n_2 \geq \cdots \geq n_s \geq -N \), \( \bar{n}_i = n_i \mod N_0 \);
- \( a_1p^{n_1} + a_2p^{n_2} + \cdots + a_sp^{n_s} = \gamma \);
- if \( 0 = n_1 = \cdots = n_{s_1} > \cdots > n_{s_r+1} = \cdots = n_s \), then \( \eta(n_1, \ldots, n_s) = (s_1! \ldots (s_r - s_{r-1})!)^{-1} \); otherwise, \( \eta(n_1, \ldots, n_s) = 0 \).
Theorem 1.2. For any \( v \geq 0 \), there is \( N^*(v) \) such that if \( N \geq N^*(v) \) 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 \( \mathcal{F}_{\gamma,N}^0 \) with \( \gamma \geq v \).

The appropriate theorem in the contravariant setting was obtained in [3] and uses the elements \( \mathcal{F}_{\gamma,N}^0 \) given by the same formula but with the factor \((-1)^{s-1}\). Indeed, when switching to the covariant setting all commutators of the form \([...[D_1,D_2],...D_s]\) should be replaced by \([D_s,...,[D_2,D_1]...]=(-1)^{s-1}[...[D_1,D_2],...D_s] \).

2. The groups \( \mathcal{G}_{h_0} \) and \( \mathcal{G}_{h_0} \)

2.1. Automorphisms \( \text{Aut}(\mathcal{K},c_0) \), \( c_0 \in p\mathbb{N} \).

Definition. For \( c_0 \in p\mathbb{N} \), let \( \text{Aut}(\mathcal{K},c_0) \) be the set of all continuous automorphisms \( h \) of \( \mathcal{K} \) such that \( h|_k = \text{id} \) and \( h(t) = t(1 + \varepsilon^p) \) with \( \varepsilon \in t^{1/p}O_k^* \).

Let \( \overline{\exp}(X) = \sum_{0 \leq i < p} X^i/i! \) be the truncated exponential. The following property can be verified by a direct calculation.

Proposition 2.1. If \( h_1, h_2 \in \text{Aut}(\mathcal{K},c_0) \) then there are \( \varepsilon_1, \varepsilon_2 \in t^{1/p}O_k^* \) such that for \( i = 1, 2 \), \( h_i(t) \equiv t \overline{\exp}(\varepsilon_i^p) \mod \text{t}^{1+\text{cop}} \) and

\[
\varepsilon_2 = \varepsilon_1 + \varepsilon_2^p \mod \text{t}^{1+\text{cop}}.
\]

2.2. Specification of a lift \( \hat{h}_0 \). It will be convenient below to specify a lift \( \hat{h}_0 \in \text{Aut}\mathcal{K}_{<p} \) of \( h_0 \) using the formalism of nilpotent Artin-Schreier theory as follows.

Definition. For \( m \in \mathbb{Z} \), an element \( b \in \mathcal{L}_k \) satisfies the condition \( C(m) \) if \( b \) is a \( k \)-linear combination of the monomials of the form \( t^{-a}[...[D_{a_1\gamma_1}, D_{a_2\gamma_2}],...D_{a_r\gamma_r}] \), where \( a \in \mathbb{Z} \) and \( a_1 + ... + a_r \geq a + m \).

Let \( \mathcal{L}_k(C(m)) \) be the subset of elements of \( \mathcal{L}_k \) satisfying the condition \( C(m) \). Then \( \mathcal{L}_k(C(0)) \) is a Lie subalgebra of \( \mathcal{L}_k \) and for any \( m \geq 0 \), \( \mathcal{L}_k(C(m)) \) is an ideal in \( \mathcal{L}_k(C(0)) \).

Define the continuous \( \mathbb{F}_p \)-linear operators \( \mathcal{R}, \mathcal{S} : \mathcal{L}_k \rightarrow \mathcal{L}_k \) as follows.

Suppose \( \alpha \in \mathcal{L}_k \).

If \( n > 0 \) then set \( \mathcal{R}(t^n\alpha) = 0 \) and \( \mathcal{S}(t^n\alpha) = -\sum_{i \geq 0} \sigma^i(t^n\alpha) \).

For \( n = 0 \), set \( \mathcal{R}(\alpha) = \alpha_0 \text{Tr}_{k/p} \alpha, \quad \mathcal{S}(\alpha) = \sum_{0 \leq i < j < N_0} \sigma^i \alpha_0 \sigma^j \alpha \).

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

The proof of the following lemma is straightforward.

Lemma 2.2. For any \( b \in \mathcal{L}_k \).

a) \( b = \mathcal{R}(b) + (\sigma - \text{id})(\mathcal{S}(b)) \);

b) \( \mathcal{R}(b) = \sum_{a \in \mathbb{Z}^+(p)} t^{-a} \mathcal{L}_k + \alpha_0 \mathcal{L} \);

c) for any \( m \), the operators \( \mathcal{R} \) and \( \mathcal{S} \) map \( \mathcal{L}_k(C(m)) \) to \( \mathcal{L}_k(C(m)) \).
Remark. The definition of the above operators \( \mathcal{R} \) and \( \mathcal{S} \) in the cases \( n > 0 \) and \( n < 0 \) is self-explanatory. In the case \( n = 0 \) we have the following picture behind. For \( \alpha \in \mathcal{L}_k \) and \( 0 \leq i < N_0 \), set \( \mathcal{R}_i(\alpha) = \alpha_0 \sigma^{-i} \alpha \) and \( \mathcal{S}(\alpha) = \sum_{0 \leq j < i} \sigma^j(\mathcal{R}_i(\alpha)) \). Then

\[
\alpha = \sum_{0 \leq i < N_0} (\sigma^i \alpha_0) \alpha = \sum_{0 \leq i < N_0} \sigma^i \mathcal{R}_i(\alpha) = \sum_{0 \leq i < N_0} ((\sigma - s \id)\mathcal{S}_i + \mathcal{R}_i) (\alpha)
\]

\[
\mathcal{R} = \sum_{0 \leq i < N_0} \mathcal{R}_i, \quad \mathcal{S} = \sum_{0 \leq i < N_0} \mathcal{S}_i,
\]

\[
\mathcal{S}(\alpha) = \sum_{0 \leq j < i < N_0} \sigma^j (\alpha_0 \sigma^{-i} \alpha) = \sum_{0 \leq j < i_1 < N_0} \sigma^j \alpha_0 \sigma^{i_1} \alpha,
\]

where \( i_1 = j - i + N_0 \). Note that there are many other ways to define \( \mathcal{S} \) in the case \( n = 0 \).

For any lift \( \hat{h}_0 \) of \( h_0 \), we have \( \hat{h}_0(f_0) = c \circ (A \otimes \id)(f_0) \), where \( c \in \mathcal{L}_K \) and \( A = \Ad(\hat{h}_0) \in \text{Aut} \mathcal{L} \) can be found from the relation

\[
(2.1) \quad h_0(\epsilon_0) \circ c = (\sigma c) \circ (A \otimes \id)(\epsilon_0),
\]

cf. Subsection \( \ref{sec:2.2} \). This allows us to specify \( \hat{h}_0 \) step by step proceeding from \( h_0 \mod C_s(\mathcal{L}) \) to \( \hat{h}_0 \mod C_{s+1}(\mathcal{L}) \), \( 1 \leq s < p \).

Indeed, suppose \( c \) and \( A \) are already chosen modulo \( s \)-th commutators. Then \( c = c' + X_s \) and \( A = A' + A_s \), where \( \deg c' < s \), \( \deg X_s \geq s \) and for any \( a \in \mathbb{Z}^0(p) \), \( \deg A'(D_{a0}) < s \) and \( \deg A_s(D_{a0}) \geq s \). (The degrees come from the Lie algebra \( \tilde{\mathcal{L}} \) uniquely determined by setting \( \deg(D_{a0}) = 1 \) for all \( a \in \mathbb{Z}^0(p) \).) Then \( \text{(2.1)} \) implies that

\[
\sigma X_s - X_s + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} A_s(D_{a0}) \equiv 0
\]

\[
h_0(\epsilon_0) \circ c' - \sigma c' \circ (A' \otimes \id)\epsilon_0 \mod C_{s+1}(\mathcal{L}_K)
\]

Now the lift \( \hat{h}_0 \) modulo \((s+1)\)-th commutators can be specified by setting \( \sum_{a \in \mathbb{Z}^0(p)} t^{-a} A_s(D_{a0}) = \mathcal{R}(B_s) \) and \( X_s = \mathcal{S}(B_s) \), where \( B_s \) is the right-hand side of the above recurrent relation.

2.3. The group \( \tilde{G}_{h_0} \). For \( h_0 \in \text{Aut}(\mathcal{K}, c_0) \), denote by \( \tilde{G}_{h_0} \) the group of all continuous automorphisms \( h \) of \( \mathcal{K}_{<p} := \mathcal{K}_{\text{sep}}^{\mathcal{L}_K(\mathcal{G})} \) such that \( h|_{\mathcal{K}} \in \langle h_0 \rangle \) — the closed subgroup in \( \text{Aut} \mathcal{K} \) generated by \( h_0 \).

Use the identification \( \eta_0 \) from Subsection \( \ref{sec:2.3} \) to obtain a natural short exact sequence of profinite \( p \)-groups

\[
(2.2) \quad 1 \longrightarrow \mathcal{G}(\mathcal{L}) \longrightarrow \tilde{G}_{h_0} \longrightarrow \langle h_0 \rangle \longrightarrow 1
\]

For any \( s \geq 2 \), \( C_s(\tilde{G}_{h_0}) \) is a subgroup in \( \mathcal{G}(\mathcal{L}) \) and, therefore, \( C_s(\tilde{G}_{h_0}) := \mathcal{L}_{h_0}(s) \) is a Lie subalgebra of \( \mathcal{L} \). Set \( \mathcal{L}_{h_0}(1) = \mathcal{L} \). Note that for any \( s_1, s_2 \geq 1 \), we have \( [\mathcal{L}_{h_0}(s_1), \mathcal{L}_{h_0}(s_2)] \subset \mathcal{L}_{h_0}(s_1 + s_2) \).

Define the weight filtration \( \mathcal{L}(s) \), \( s \in \mathbb{N} \), in \( \mathcal{L} \) by setting \( \text{wt}(D_{a0}) = s \) if \((s-1)c_0 \leq a < sc_0 \). With this notation \( \mathcal{L}(s)_k \) is generated over \( k \) by
all \([\ldots [D_{a_1n_1}, D_{a_2n_2}], \ldots, D_{a_rn_r}]\) such that \(\sum_i \text{wt}(D_{a_in_i}) \geq s\). For any \(s_1, s_2 \geq 1\), we also have that \([\mathcal{L}(s_1), \mathcal{L}(s_2)] \subset \mathcal{L}(s_1 + s_2)\).

**Theorem 2.3.** For all \(s \in \mathbb{N}\), \(\mathcal{L}_{h_0}(s) = \mathcal{L}(s)\).

*Proof.* Note that \(\mathcal{L}_{h_0}(2)\) is generated by the elements of \(C_2(\mathcal{L})\) and the commutators \((\hat{h}_0, l) = (-l) \circ \text{Ad}(\hat{h}_0)(l)\), where \(l \in \mathcal{L}\) and \(h_0\) is a lift of \(h_0\). Then the identity

\[
(-Y) \circ (X + Y) \equiv X \text{ mod } [X, \mathcal{L}]
\]

implies (with \(X = \text{Ad}(\hat{h}_0)(l) - l\) and \(Y = l\)) that

\[
(-l) \circ \text{Ad}(\hat{h}_0)(l) \equiv (\text{Ad}(\hat{h}_0) - \text{id})(l) \text{ mod } [\text{Ad}(\hat{h}_0)(l) - l, \mathcal{L}]
\]

Therefore, \(\mathcal{L}_{h_0}(2)\) is generated by \(C_2(\mathcal{L})\) and all \((\text{Ad}(\hat{h}_0) - \text{id})(l)\), \(l \in \mathcal{L}\). Similarly, for any \(s \geq 2\), \(\mathcal{L}_{h_0}(s)\) is generated by the elements of the form \((\text{Ad}(\hat{h}_0) - \text{id})^s(l)\), where \(l \in C_s(\mathcal{L})\), \(s_1, s_2 \geq 1\) and \(s_1 + s_2 \geq s\).

Suppose \(n \in \mathbb{Z}^+(p)\) and \(\text{Ad}(\hat{h}_0)(D_{a_0}) - D_{a_0} = l_1(D_{a_0}) + l_2(D_{a_0}) \in \mathcal{L}_{k}\), where \(l_1(D_{a_0})\) is a linear part (with respect to the generators \(\{D_{an} | a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{D_0\}\)) and \(l_2(D_{a_0})\) is a linear combination of commutators of order \(\geq 2\).

**Lemma 2.4.** If \(\hat{h}_0\) is the lift from Subsection 2.2 then:

- a) \(l_1(D_{a_0}) = \sum_{n,b} \alpha_{bn}(a) D_{bn}\), where all \(\alpha_{bn}(a) \in k\) and \(\alpha_{bn}(a) = 0\) if \(b < a + c_0\);
- b) if \(n \not\equiv 0 \text{ mod } N_0\) then \(\alpha_{an}(a) = 0\) and \(\alpha_{a0}(a) \neq 0\);
- c) \(l_2(D_{a_0})\) is a \(k\)-linear combination of \([\ldots [D_{a_1n_1}, D_{a_2n_2}], \ldots, D_{a_rn_r}]\), where \(r \geq 2\) and \(a_1 + \ldots + a_r \geq a + c_0\).

*Proof.* Clearly, \(h_0(c_0) - c_0\) satisfies the condition \(C(c_0)\).

Consider the recursion relation from the end of Subsection 2.2. By induction on \(s\) we can assume that \(c^r\) satisfies the condition \(C(c_0)\). Then the right-hand side of that relation belongs to \(\mathcal{L}_k(C(c_0))\). Therefore, \(X_s\) and \(\sum_{\alpha \in \mathbb{Z}^+(p)} t^{-\alpha} D_{a_0}\) also belong to \(\mathcal{L}_k(C(c_0))\) (use Lemma 2.2). So, \(c \in \mathcal{L}_k(C(c_0))\) and \(\sum_{\alpha \in \mathbb{Z}^+(p)} t^{-\alpha}(a \otimes \text{id})(D_{a_0}) \equiv c_0 \text{ mod } \mathcal{L}_k(C(c_0))\).

In particular, we proved the properties a) and c) of our lemma. Part b) is obtained by direct calculation.

**Lemma 2.5.** Suppose \(\hat{h}_0\) is the lift from Subsection 2.2. If \(s \in \mathbb{N}\) and \(\text{wt}(D_{a_0}) \geq s\) then \(\text{wt}(\text{Ad}(\hat{h}_0)(D_{a_0}) - D_{a_0}) \geq s + 1\).

*Proof.* By Lemma 2.4 it will be sufficient to verify that the inequality \(a_1 + \ldots + a_r \geq a + c_0\) implies that

\[
\text{wt}([\ldots [D_{a_1n_1}, D_{a_2n_2}], \ldots, D_{a_rn_r}]) \geq s + 1.
\]

Indeed, if for all \(i, (s_i - 1)c_0 \leq a_i < s_ic_0\) then

\[
(s_1 + \ldots + s_r)c_0 > a_1 + \ldots + a_r \geq a + c_0 \geq sc_0
\]

and \(\text{wt}(D_{a_1n_1} \ldots D_{a_rn_r}) = s_1 + \ldots + s_r > s\).
By Lemma 2.5 for any $s_1, s_2 \in \mathbb{N}$ such that $s_1 + s_2 \geq s$ and any $l \in C_{s_2}(\mathcal{L})$, we have $(\text{Ad}(\hat{h}_0) - \text{id})^{s_1}(l) \in \mathcal{L}(s)$. Therefore, $\mathcal{L}_{h_0}(s) \subset \mathcal{L}(s)$.

It remains to verify that

- if $\text{wt}(D_{a_0}) = s$ then $D_{a_0} \in \mathcal{L}_{h_0}(s)$.

This is obvious for $s = 1$ and we can use induction on $s$.

If $\text{wt}(D_{a_0}) = s + 1$ then $\text{wt}(D_{a-c_0,0}) = s$, $D_{a-c_0,0} \in \mathcal{L}_{h_0}(s)$ and

$$\text{Ad}(\hat{h}_0)(D_{a-c_0,0}) - D_{a-c_0,0} \in \mathcal{L}_{h_0}(s + 1).$$

Consider $l_2(D_{a-c_0,0})$ from Lemma 2.4.

By inductive assumption $l_2(D_{a-c_0,0}) \in \mathcal{L}_{h_0}(s + 1)$. This implies that $l_2(D_{a-c_0,0}) \in \mathcal{L}_{h_0}(s + 1)$ and (use that $\alpha_{a-c_0,0}(a - c_0) \neq 0$) $D_{a_0} \in \mathcal{L}_{h_0}(s + 1)$. The theorem is proved. □

2.4. The group $G_{h_0}$. Let $G_{h_0} = \tilde{G}_{h_0}/G_{h_0} C_p(\tilde{G}_{h_0})$.

**Proposition 2.6.** Exact sequence (2.2) induces the following exact sequence of $p$-groups

$$1 \longrightarrow G(\mathcal{L})/G(\mathcal{L}(p)) \longrightarrow G_{h_0} \longrightarrow \langle h_0 \rangle \text{ mod } \langle h_0^p \rangle \longrightarrow 1$$

**Proof.** Set

$$\mathcal{M}_K = \sum_{1 \leq s < p} t^{-c_0s} \mathcal{L}(s)_{m_K} + \mathcal{L}(p)_{K}$$

$$\mathcal{M}_{K_{\text{sep}}} = \sum_{1 \leq s < p} t^{-c_0s} \mathcal{L}(s)_{m_{\text{sep}}} + \mathcal{L}(p)_{K_{\text{sep}}}$$

where $m_K$ and $m_{\text{sep}}$ are the maximal ideals of the valuation rings of $K$ and, resp., $K_{\text{sep}}$. Then $\mathcal{M}_K$ is a Lie subalgebra in $\mathcal{L}_K$ and $t^{c_0(p-1)}\mathcal{M}_K$ is an ideal in $\mathcal{M}_K$. Similarly, $\mathcal{M}_{K_{\text{sep}}}$ is a Lie subalgebra in $\mathcal{L}_{K_{\text{sep}}}$ and $t^{c_0(p-1)}\mathcal{M}_{K_{\text{sep}}}$ is its ideal. Note that $\mathfrak{e}_0 \in \mathcal{M}_K$, $f_0 \in \mathcal{M}_{K_{\text{sep}}}$,

$$t^{c_0(p-1)}\mathcal{M}_{K_{\text{sep}}} \cap \mathcal{M}_K = t^{c_0(p-1)}\mathcal{M}_K,$$

and we have a natural embedding of $\tilde{M}_K := \mathcal{M}_K/t^{c_0(p-1)}\mathcal{M}_K$ into $\tilde{M}_{K_{\text{sep}}} := \mathcal{M}_{K_{\text{sep}}}/t^{c_0(p-1)}\mathcal{M}_{K_{\text{sep}}}$. For $i \geq 0$, we have also that $(\tilde{h}_0 - \text{id})^i\mathcal{M}_K = (t^{c_0} \mathcal{M}_K$ and $(\tilde{h}_0 - \text{id})^i\mathcal{M}_{K_{\text{sep}}} = t^{i c_0} \mathcal{M}_{K_{\text{sep}}}$.

Consider the orbit of $\tilde{f}_0 := f_0 \text{ mod } t^{c_0(p-1)}\mathcal{M}_{K_{\text{sep}}}$ with respect to the natural action of $\tilde{G}_{h_0} \subset \text{Aut } K_{\text{sep}}$ on $\mathcal{M}_{K_{\text{sep}}}$. Our Proposition will be proved if we verify that the stabilizer $\mathcal{H}$ of $\tilde{f}_0$ equals $\tilde{G}_{h_0}/C_p(\tilde{G}_{h_0})$.

If $l \in \mathcal{L}$ then $l : f_0 \mapsto f_0 \circ l$. This implies that if $l \in \mathcal{L} \cap \mathcal{H}$ then $l \in L(p)_{K_{\text{sep}}} \cap \mathcal{L} = L(p) = C_p(\tilde{G}_{h_0})$. Therefore, $\mathcal{H} \cap G(\mathcal{L}) = C_p(\tilde{G}_{h_0})$.

Note that $\tilde{G}_{h_0} \text{ mod } C_p(\tilde{G}_{h_0})$ is generated by $\tilde{h}_0^p$. This follows from the fact that the subset of $p$-th powers in any $p$-group of nilpotent class $< p$ forms a subgroup.

Now we use that $\tilde{h}_0(f_0) = c \circ (a \otimes \text{id})(f_0)$, where $c \in G(\mathcal{L}_K)$ and $a = \text{Ad}(\hat{h}_0)$. Then

$$\tilde{h}_0(f_0) = h_0^{-1}(c \circ (a \otimes h_0^{-1})c \circ \cdots \circ (a \otimes h_0^{-1})^{p-1}c) \circ (a^p \otimes \text{id})f_0$$
Automorphisms of period \( p \) and nilpotent class \( < p \)

Clearly, \((a - \text{id})^p \mathcal{L} \subset \mathcal{L}(p)\) and, therefore, \((a^p \otimes \text{id}) \bar{f}_0 = \bar{f}_0\). Also note that for \( s \geq 0 \), \((a \otimes h_0^{-1} - \text{id})(t^{(s+1)} \mathcal{M}_K) \subset t^{(s+1)} \mathcal{M}_K\). Therefore, \(\psi := a \otimes h_0^{-1}\) is an automorphism of \(G_1(\mathcal{M}_K)\) of order \( p \). We have the following property of \( p \)-groups with nilpotent class \( < p \).

**Lemma 2.7.** Suppose \( H \) is a \( p \)-group of nilpotent class \( < p \) and period \( p \) and \( \psi \) is an automorphism of \( H \) of order \( p \). Then for any \( h \in H \), \( h\psi(h) \ldots \psi^{p-1}(h) = e\).

**Proof of Lemma.** Let \( G \) be a semi-direct product of \( H \) and \( \mathbb{Z}/p \) via \( \psi \), i.e. \( G = \{(h, m) \mid h \in H, m \in \mathbb{Z}/p\}\) and the composition law in \( G \) is defined via \((h_1, m_1)(h_2, m_2) = (h_1 \psi^m(h_2), m + n)\). Then \( G \) has nilpotent class \( < p \) and, therefore, it is a group of period \( p \). (Use that the product of \( p \)-th powers in a group of nilpotent class \( < p \) is again a \( p \)-th power, [17], Subsection 12.3.). Then

\[(e, 0) = (h, 1)^p = (h\psi(h) \ldots \psi^{p-1}h, 0).\]

Continue the proof of our proposition. The above lemma implies that \( c \circ \psi(c) \circ \cdots \circ \psi^{p-1}(c) = 0\), i.e. \( h_0^p(\bar{f}_0) = \bar{f}_0\). Thus, we proved that \( \mathcal{G}^p_{\eta_0} C_p(\mathcal{G}_{\eta_0}) \subset \mathcal{H} \).

Suppose \( g = h_0^l \in \mathcal{H} \) with some \( l \in G(\mathcal{L}) \). Then \( g(\bar{f}_0) = m \circ f_0\) where \( m \in t^{(s+1)} \mathcal{M}_K, \sigma(m) \in t^{(s+1)} \mathcal{M}_K \) and \( g(e_0) \circ m \circ f_0 = g(e_0) \circ g(f_0) = g(\sigma f_0) = \sigma m \circ \sigma f_0 = \sigma m \circ e_0 \circ f_0\) implies that \( g(e_0) \equiv e_0 \mod t^{(s+1)} \mathcal{M}_K\). Thus \( h_0^k(e_0) \equiv e_0 \mod t^{(s+1)} \mathcal{M}_K, k \equiv 0 \mod p \) (use that \( h_0 \in \text{Aut}(K), c_0 \) and \( p > 2 \)) and \( l \in \mathcal{H} \cap \mathcal{L} = \mathcal{L}(p) = C_p(\mathcal{G}_{\eta_0}) \). The proposition is proved.

**Corollary 2.8.** If \( L \) is an \( \mathbb{F}_p \)-Lie algebra such that \( \mathcal{G}_{\eta_0} = G(L) \) then \([2.3]\) induces the following short exact sequence of Lie \( \mathbb{F}_p \)-algebras

\[0 \rightarrow \mathcal{L}/\mathcal{L}(p) \rightarrow L \rightarrow \mathbb{F}_p h_0 \rightarrow 0\]

2.5. Ramification estimates. Use the identification from Subsection \([3]\) \( \eta_0 : \text{Gal}(K_{\leq p}/K) \simeq G(\mathcal{L}) \) and set for \( s \in \mathbb{N}, K[s] := K_{\leq p}^{[\mathcal{L}(s+1)]:} \). Denote by \( v[s] \) the maximal upper ramification number of the extension \( K[s]/K \). In other words,

\[v[s] = \max\{v \mid \Gamma^{(v)}_K \text{ acts non-trivially on } K[s]\} \text{.}\]

Note, if \( 1 \leq s < p \) then \( v[s] \) is the maximal upper ramification number of the maximal \( p \)-extension of \( K \) with Galois group of period \( p \) and nilpotence class \( s \).

**Proposition 2.9.** For all \( s \in \mathbb{N}, v[s] = c_0 s - 1\).

**Proof.** Remind that for any \( v \geq 0, \pi f_0(e_0)(G^{(v)}) = L^{(v)} \) and for sufficiently large \( N \), the ideal \( L_{\eta}^{(v)} \) is generated by all \( \sigma^n f^0_{\gamma, -N} \), where \( \gamma \geq v, n \in \mathbb{Z} \) and the elements \( f^0_{\gamma, -N} \) were given in Subsection \([3]\).
Note that $L^{(v)}$ is contained in the ideal generated by the monomials $a^v[a_1, a_2n_2, \ldots, a_vn_v]$ such that $\max\{n_1, \ldots, n_v\} = 0$ and $a_1p^n + \cdots + a_vp^n > v$. So, $v < a_1 + \cdots + a_v \leq c_0\text{wt}(D_{a_1n_1} \ldots D_{a_vn_v}) - r_0$ where $r_0$ is the number of non-zero $a_i$'s.

If $v > c_0s - 1$ then $\text{wt}([\ldots [D_{a_1n_1}, D_{a_2n_2}], \ldots D_{a_vn_v}]) > s$ and we have $L^{(v)}(s) \subset L(s)$. If $v = c_0s - 1$ then $\text{wt}([\ldots [D_{a_1n_1}, D_{a_2n_2}], \ldots D_{a_vn_v}]) \leq s$ if $r_0 = 1$ and the only non-zero $a_i$ equals $c_0s - 1$. Therefore, $L^{(v)}(s+1)$ is generated by the images of $D_{c_0s-1,n}, n \in \mathbb{Z}/N_0$, and $L^{(v)} \not\subset L(s+1)$. □

3. Structure of Lie algebra $L$

The group structure of $G(L)$, cf. Corollary 2.8, is given via the conjugation $\text{Ad}(\hat{h}_0)$ on $G(L/L(p))$, where $\hat{h}_0$ is a chosen lift of $h_0$. This conjugation appears as a unipotent automorphism of the Lie algebra $L/L(p)$. Then $\text{Ad}(\hat{h}_0) = \exp(\text{ad}(\hat{h}_0))$ because $L(p)$ has nilpotent class $< p$. So, the knowledge of $L$ is equivalent to the knowledge of the differentiation $\text{ad}(h_0)$ of $L/L(p)$ and this differentiation comes from a differentiation of $L$. (Use that $L$ is a free object in the category of Lie $\mathbb{F}_p$-algebras of nilpotent class $< p$.)

3.1. Unipotent actions in characteristic $p$. Suppose $F$ is a field of characteristic $p$. Let $u$ be a variable and let $\mathbb{G}_a,F = \text{Spec} F[u]$ be the (additive) group scheme over $F$ with the coaddition $\Delta(u) = u \otimes 1 + 1 \otimes u$. It acts on an $F$-module $\mathcal{M}$ if there is an $F$-linear morphism $s : \mathcal{M} \rightarrow \mathcal{M} \otimes F[u]$ such that for any $m \in \mathcal{M}$, $s(m)|_{u=0} = m$ and $(s \otimes \text{id})s = (\text{id} \otimes \Delta)s$. In particular, for $i \geq 0$, there are $F$-linear morphisms $s_i : \mathcal{M} \rightarrow \mathcal{M}$ such that $s(m) = \sum_{i \geq 0} s_i(m) \otimes u^i$. The morphism $m \mapsto s_1(m) \otimes u$ will be denoted sometimes by $ds$. From the definition of $s$ it follows that for any $0 \leq i < p$, $s_i(m) = s_1(m)/i!$. Therefore, the action $s$ is completely determined by its “linearization” $ds$ via $s = \exp(ds)$. This will allow us to describe below the action of the cyclic group $\langle \hat{h}_0 \rangle \mathbb{Z}/p$ on the $p$-group $G(L/L(p))$ by the differentiation $\text{ad} \hat{h}_0$ of the Lie $\mathbb{F}_p$-algebra $L/L(p)$. The appropriate formalism is provided by the following Proposition.

Proposition 3.1. Suppose the cyclic group $\langle \tau \rangle \mathbb{Z}/p$ acts on an $F$-module $\mathcal{M}$ and for $i \geq 0$, $\mathcal{M}_i = (\tau - \text{id})^i \mathcal{M}$. Then there is an action $s : \mathcal{M} \rightarrow \mathcal{M} \otimes F[u]$ of $\mathbb{G}_a,F$ on $\mathcal{M}$ such that for any $m \in \mathcal{M}$:

a) if $i \in \mathbb{Z}/p$ then $\tau^i(m) = s(m)|_{u=i}$;

b) if $m \in \mathcal{M}_k$ then $s_i(m) \in \mathcal{M}_{k+i}$, in particular, for $i \geq p$, $s_i = 0$.

Proof. We have $\mathcal{M} = \mathcal{M}_0 \supset \mathcal{M}_1 \supset \cdots \supset \mathcal{M}_{p-1} \supset \mathcal{M}_p = 0$.

For any $m \in \mathcal{M}$, there are unique $s_i(m) \in \mathcal{M}$, $0 \leq i \leq p-1$, such that for all $k \in \mathbb{Z}/p$, $\tau^k(m) = \sum_{i} s_i(m) \otimes u^i|_{u=k}$. (Use that $\det(k^i)_{0 \leq i, k \leq p-1} \neq 0$.)
Let \( s(m) = \sum s_i(m) \otimes u^i \).
Clearly, \( s(m)(0) = s_0(m) = m \).

Then \( m \mapsto s(m) \) gives an \( \mathbb{F}_p \)-linear map \( s : \mathcal{M} \to \mathcal{M} \otimes \mathbb{F}_p[u] \). The polynomials \( (s \otimes \text{id})s(m)(u \otimes 1, 1 \otimes u) \) and \( (\text{id} \otimes \Delta)s(m)(u \otimes 1, 1 \otimes u) \) coincide in the points \((u_1, u_2)\) such that \( 0 \leq u_1, u_2, u_1 + u_2 < p \). Note that the second polynomial has the total degree \( < p \). If we establish the similar property for the first polynomial then these polynomials must identically coincide and our proposition will be proved.

**Lemma 3.2.** If \( i_0 \geq 0, m \in \mathcal{M}_{i_0} \) then for any \( i \geq 0 \), \( s_i(m) \in \mathcal{M}_{i_0+i} \).

**Proof.** For \( i \geq 0 \) and \( F \in \mathcal{M} \otimes \mathbb{F}_p[u] \), define the \( i \)-th differences \( (\Delta^i F)(u) \in \mathcal{M} \otimes \mathbb{F}_p[u] \) by setting \( \Delta^0 F = F \) and

\[
(\Delta^{i+1} F)(u) = (\Delta^i F)(u + 1) - (\Delta^i F)(u).
\]

In particular, for \( 0 \leq j < i \), \( \Delta^i(1 \otimes u^j) = 0 \) and \( (\Delta^i)(1 \otimes u^j) = i! \). Therefore, for any \( i \geq 0 \),

\[
(\Delta^i s(m)|_{u=0} = i! s_i(m) + \sum_{j > i} f_{ij} s_j(m)|_{u=0}
\]

where all \( f_{ij} \in F \).

Note that for every value \( 0 \leq u_0 < p \),

\[
\Delta^1 s(m)|_{u=u_0} = \tau(s(m)|_{u=u_0}) - s(m)|_{u=u_0} \in \mathcal{M}_{i_0+1},
\]

\[
\Delta^2 s(m)|_{u=u_0} = \tau(\Delta^1 s(m)|_{u=u_0}) - \Delta^1 s(m)|_{u=u_0} \in \mathcal{M}_{i_0+2}
\]

and so on. Therefore, \( \Delta^{p-i_0}s(m)|_{u=0} = (p - i_0)! s_{p-i_0}(m) \in \mathcal{M}_p = 0 \) implies that \( s_{p-i_0}(m) = 0 \). Then relation (3.1) implies by descending induction the statement of our lemma.

It remains to note now that \( (s \otimes \text{id})s(m) \) is equal to

\[
m \otimes 1 \otimes 1 + \sum_{1 \leq i < p} s_i(m)(u^i \otimes 1 + 1 \otimes u^i) + \sum_{1 \leq i,j < p} s_i(s_j(m)) \otimes u^j \otimes u^i
\]

and by the above lemma, \( s_i(s_j(m)) = 0 \) if \( i + j \geq p \).

The proposition is proved.

3.2. **The morphisms** \( \text{ad} \hat{h}_0 \). Apply the approach from Subsection 3.1 to describe the action of the lift \( \hat{h}_0 \) on \( \mathcal{M}_{K_{\text{sep}}} \) in terms related to the Lie algebra \( \mathcal{L} \).

As earlier, let \( \hat{h}_0(f_0) = c \circ (\text{Ad}(\hat{h}_0) \otimes \text{id})f_0 \), where \( c \in \mathcal{L}_K \). For \( 1 \leq i < p \), let \( \hat{h}_0^i(f_0) = c(i) \circ f_0(i) \), where

\[
c(i) = (\text{id} \otimes h_0^{i-1})c \circ (\text{Ad}h_0 \otimes h_0^{i-2}) \circ \cdots \circ (\text{Ad}^{i-1}h_0 \otimes \text{id})c
\]

and \( f_0(i) = (\text{Ad}^i \hat{h}_0 \otimes \text{id})f_0 \).

Introduce \( c[u] \in \mathcal{L}_K \otimes \mathbb{F}_p[u] \) and \( f_0[u] \in \mathcal{L}_{K_{\text{sep}}} \otimes \mathbb{F}_p[u] \) such that for \( 0 \leq k < p \), \( c[u]|_{u=k} = c(k) \) and \( f_0[u]|_{u=k} = f_0(k) \). Then

\[
c[u] = c_0 \otimes 1 + c_1 \otimes u + \cdots + c_{p-1} \otimes u^{p-1}
\]
where \( c_0 = 0 \) and for \( i \geq 1, c_i \in t^{ca} \mathcal{M}_K \). We have also
\[
f[u] = f_0 \otimes 1 + f_1 \otimes u + \cdots + f_p \otimes u^{p-1},
\]
where all \( f_i \in t^{ca} \mathcal{M}_{K_{sep}} \).

With the above notation the action of \( (\hat{h}_0)^{\mathbb{Z}/p} \) on \( \tilde{\mathcal{M}}_{K_{sep}} \) appears as
the action of the group scheme \( \mathbb{G}_{a,F_p} \) via the following map
\[
\hat{h}_0^a : \tilde{f}_0 \mapsto c[u] \circ f_0[u] = (c_1 u + \ldots) \circ (f_0 + f_1 u + \ldots) \mod t^{ca(p-1)} \mathcal{M}_{K_{sep}}.
\]
These data are related as follows
\[
(3.2) \quad \hat{h}_0^a(\varepsilon_0) \circ c[u] = \sigma c[u] \circ \sum_{a \in \mathbb{Z}^n(p)} t^{-a} \text{Ad}(\hat{h}_0^a)(D_{a0})
\]
Note that \( \text{Ad}(\hat{h}_0^a) \equiv \text{id} + \text{ad}(\hat{h}_0)u \mod u^2 \) and \( \sigma u = u \). Now we can specify the lift \( \hat{h}_0(e_0) \) as follows.

Remind, cf. Subsection 2.1 that \( h_0 \in \text{Aut}(K, c_0) \), i.e. there is an \( \varepsilon_0 \in t^{ca/p}O_K^\times \) such that \( h_0(t) = t \exp(\varepsilon_0^p) \mod t^{pc_0+1} \). Then by Proposition 2.1 we have \( \hat{h}_0^a(t) = t \exp(u \varepsilon_0^p) \mod t^{pc_0+1} \). Therefore,
\[
d\hat{h}_0^a(e_0) = \sum_{a \in \mathbb{Z}^n(p)} t^{-a} \varepsilon_0^p a D_{a0}u.
\]

**Proposition 3.3.** We have the following recurrent relation for \( c_1 \) and \( V_a = \text{ad} \hat{h}_0(D_{a0}), a \in \mathbb{Z}^0(p) \),
\[
(3.3) \quad \sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^n(p)} t^{-a} V_a =
\]
\[
\sum_{k \geq 1} \frac{1}{k!} t^{-(a_1 + \cdots + a_k)} \varepsilon_0^p \cdot [a_1 D_{a_10}, D_{a_20}, \ldots, D_{a_k0}]
\]
\[
- \sum_{k \geq 2} \frac{1}{k!} t^{-(a_1 + \cdots + a_k)} \cdot [V_{a_1}, D_{a_20}, \ldots, D_{a_k0}]
\]
\[
- \sum_{k \geq 1} \frac{1}{k!} t^{-(a_1 + \cdots + a_k)} \cdot [\sigma c_1, D_{a_10}, \ldots, D_{a_k0}]
\]
The indices \( a_1, \ldots, a_k \) in all above sums run over \( \mathbb{Z}^0(p) \).

**Proof.** Suppose \( X \) and \( Y \) are generators of a free Lie \( \mathbb{F}_p[u] \)-algebra of nilpotent class \( < p \). Then, cf. Subsection 4.4 in [13]:
\[
(3.4) \quad X + uY = X \circ \left( u \sum_{k \geq 1} \frac{1}{k!} \left[ \cdots [Y, X], \ldots, X \right] \right) \mod u^2
\]
\[
(3.5) \quad (uY) \circ X = X \circ \left( u \sum_{k \geq 0} \frac{1}{k!} \left[ \cdots [Y, X], \ldots, X \right] \right) \mod u^2
\]
The left-hand side of (3.2) equals
\[ (e_0 + \hat{d}h_0^0(e_0) + \ldots) \circ (c_1 u + \ldots) = e_0 \circ \left( \sum_{k \geq 1} \frac{1}{k!} \ldots [\hat{d}h_0^0(e_0), e_0], \ldots, e_0] + c_1 u \right) \]

Similarly, the right-hand side of (3.2) is equal to
\[ (\sigma c_1 u + \ldots) \circ (e_0 + u \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a + \ldots) = e_0 \circ \left( u \sum_{k \geq 1} \ldots [V_a, e_0], \ldots, e_0] + u \sum_{k \geq 0} \frac{1}{k!} \ldots [\sigma c_1, e_0], \ldots, e_0] + \ldots \right) \]

It remains to cancel by \( e_0 \) and equalize the coefficients for \( u \) in the formulas inside the big brackets. \( \Box \)

3.3. Special cases. Recurrent relation (3.3) describes explicitly step by step the action of the lift \( \hat{h}_0 \) of \( h_0 \). We can agree, for example, to find on each step the appropriate values of \( c_1 \) and \( V_a \) by the use of operators \( R \) and \( S \) from Subsection 2.2. This will specify uniquely the lift \( \hat{h}_0 \) together with its action on \( L/\mathfrak{L}(p) \) and, therefore, will determine the structure of \( L \) (and of the group \( \mathcal{G}_{h_0} \)).

Let \( \varepsilon^0_p = \sum_{i \geq 0} A_i t^{c_0 + pi} \), where all \( A_i \in k \) and \( A_0 \neq 0 \). Then proceeding modulo \( C_2(\mathcal{L}_K) \) we obtain:
\[ \sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a = \sum_{a \in \mathbb{Z}^0(p)} A_i t^{c_0 + pi - a} a D_{i0} \mod C_2(\mathcal{L}_K) \]

This implies that
- for all \( b \in \mathbb{Z}^+(p) \), \( (\text{ad} h_0)(D_{i0}) = \sum_{i \geq 0} \alpha_i b D_{i0+c_0+pi} \);
- \( (\text{ad} h_0)(D_0) \in C_2(\mathcal{L}) \).

The first relation means that we can eliminate all \( D_{an} \) with \( a > c_0 \) from the system of minimal generators of \( L_k \). The second relation then means that \( L \) 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 \( \tilde{L}/C_p(\tilde{L}) \), where \( \tilde{L} \) 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, \( \mathcal{G}_{h_0} \) can be treated as an object of this category with finitely many generators and one relation.
We can make the first central step to obtain the following explicit formulas for $V_a = \text{ad} h_0(D_{a0})$ modulo $C_3(L_k)$:

$$V_0 \equiv \frac{1}{2} \alpha_0 \sum_{i \geq 0 \atop 0 \equiv n < N_0} \sigma^n(A_i F^0_{co+pi}, 0) \mod C_3(L_k).$$

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

$$V_a = \sum_{n \geq 1 \atop i \geq 0} \sigma^n(A_i F^0_{co+pi+a/p^n}, -n) + \frac{1}{2} \sum_{m \geq 0 \atop i \geq 0} \sigma^{-m}(A_i F^0_{co+pi+a/p^m}, 0).$$

4. Arithmetical lifts $\hat{h}_0$

4.1. Review of ramification theory. The following brief sketch of ramification theory of groups of continuous automorphisms of complete discrete valuation fields with perfect residue field is based on the papers [14, 29, 30].

Let $E$ be a complete discrete valuation field with perfect residue field $k_E$ and the maximal ideal $m_E$. Let $E_{sep}$ be a separable closure of $E$. Let $\mathcal{I}_E$ be the group of all continuous automorphisms of $E_{sep}$ which are compatible with $v_E$ and induce the identity map on the residue field of $E_{sep}$. If $F$ is a finite extension of $E$ in $E_{sep}$ then we always assume that $F_{sep} = E_{sep}$ and, therefore, obtain a natural identification $\mathcal{I}_E = \mathcal{I}_F$. Note that the inertia subgroup $\Gamma^0_E$ of $\Gamma_E = \text{Gal}(E_{sep}/E)$ is a subgroup in $\mathcal{I}_E$.

For $x \geq 0$, set

$$\mathcal{I}_{F,x} = \{ \iota \in \mathcal{I} \mid v_F(\iota(a) - a) \geq 1 + x \ \forall a \in m_F \}.$$

Denote by $\mathcal{I}_{F/E}$ the set of all continuous embeddings of $F$ into $E_{sep}$ which induce the identity map on $E$ and $k_F$. For $x \geq 0$, let

$$\mathcal{I}_{F/E,x} = \mathcal{I}_{E,x} \cap \mathcal{I}_{F/E}.$$

If $\iota_1, \iota_2 \in \mathcal{I}_{F/E}$ and $x \geq 0$ then $\iota_1$ and $\iota_2$ are $x$-equivalent iff for any $a \in m_F$, $v_F(\iota_1(a) - \iota_2(a)) \geq 1 + x$. Denote by $(\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x})$ the number of $x$-equivalent classes in $\mathcal{I}_{F/E}$. Then the Herbrand function for the field extension $F/E$ can be defined for all $x \geq 0$, as $\varphi_{F/E}(x) = \int_0^x (\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x})^{-1} dx$. This function has the following properties:

- $\varphi_{F/E}$ is a piece-wise linear function with finitely many edges;
- if $L \supset F \supset E$ is a tower of finite field extensions then for any $x \geq 0$, $\varphi_{L/E}(x) = \varphi_{F/E}(\varphi_{L/F}(x)).$

Then the ramification filtration $\{ \mathcal{I}_E^{(v)} \}_{v \geq 0}$ on $\mathcal{I}_E$ appears as a decreasing sequence of the subsets $\mathcal{I}_E^{(v)}$ of $\mathcal{I}_E$, which consists of $\iota \in \mathcal{I}_E$ such
that for any finite extension $F$ of $E$, $v \in I_{F,v(F)}$, where $\varphi_{F/E}(v(F)) = v$.

Note that $I_E^{(v)} = I_F^{(v(F))}$ and $\Gamma_E \cap I_E^{(v)}$ is the usual higher ramification subgroup $I_E^{(v)}$ of $\Gamma_E$ with the upper number $v$.

### 4.2. Arithmetical lifts.

For any $v \geq 0$, denote by $\text{Aut}^{(v)}F$ the group of continuous automorphisms $\varphi$ of $F$ such that for any $a \in m_F$, we have $v_F(\varphi(a) - a) \geq 1 + v$.

Suppose $F/E$ is a finite Galois extension in $E_{\text{sep}}$, and $h \in \text{Aut}^{(v)}E$ with the maximal possible $v$. Suppose $h$ admits a lift to $F$, i.e. there is $h' \in \text{Aut}F$ such that $h'|_E = h$. This lift will be called arithmetical if $h' \in \text{Aut}^{(v)}F$ with $\varphi_{F/E}(v') = v$. We can see easily that $v'$ is the maximal possible for $h'$.

With the above notation and assumption we have the following property.

**Proposition 4.1.**

a) If $h$ admits a lift to $F$ then it admits also arithmetical lift to $F$;

b) If $h''$ is another arithmetical lift of $h$ to $F$ then $h'' \equiv h' \mod \Gamma^{(v)}_{F/E}$

### 4.3. Characterisation of arithmetical lifts.

Suppose $h_0$ is an arithmetical lift of $h_0 \in \text{Aut}(\mathcal{K},c_0)$ to $\mathcal{K}_{\text{sep}}$. In particular, $h_0|_{\mathcal{K}_{<p}}$ is an arithmetical lift of $h_0$ to $\mathcal{K}_{<p}$. (We shall use sometimes below the simpler notation $\hat{h}_0$ instead of $h_0|_{\mathcal{K}_{<p}}$.) Clearly, $\hat{h}_0 \in I^{(c_0)}$ and $c_0$ is the maximal number with such property. Therefore, $\hat{h}_0 \in \text{Aut}^{(c_{<p})}\mathcal{K}_{<p}$, where $c_{<p} = \varphi_{\mathcal{K}_{<p}/\mathcal{K}}^{-1}(c_0)$, and $c_{<p}$ is the maximal number with such property.

By Proposition 4.1b), a lift $\hat{h}_0|_{\mathcal{K}_{<p}}$ is unique modulo $\Gamma^{(c_0)}_{\mathcal{K}_{<p}/\mathcal{K}}$. Therefore, $\hat{h}_0$ can be specified uniquely by its action on $\mathcal{M}_{\mathcal{K}_{<p}}$ modulo $t_0^{c_{<p}(p-1)} \mathcal{M}_{\mathcal{K}_{<p}} + L^{(c_0)}_{\mathcal{K}_{<p}}$. (Use that $\Gamma_{\mathcal{K}_{<p}/\mathcal{K}}$ acts strictly on $\mathcal{M}_{\mathcal{K}_{<p}} = \mathcal{M}_{\mathcal{K}_{<p}}/t_0^{c_{<p}(p-1)} \mathcal{M}_{\mathcal{K}_{<p}}$.)

Notice also that for any $g \in \Gamma_{\mathcal{K}}$, $\hat{h}_0^{-1}g\hat{h}_0 \equiv g \mod \Gamma^{(c_0)}_{\mathcal{K}}$. Therefore, $(\text{Ad}\hat{h}_0 \otimes \text{id})(f_0) \equiv f_0 \mod L^{(c_0)}_{\mathcal{K}}$ and the property for $\hat{h}_0$ to be arithmetical can be uniquely stated in terms of $c \mod (t_0^{c_{<p}(p-1)} \mathcal{M}_{\mathcal{K}} + L^{(c_0)}_{\mathcal{K}})$, where $c \in L_{\mathcal{K}}$ is such that $\hat{h}_0(f_0) = c \circ (\text{Ad}\hat{h}_0 \otimes \text{id})f_0$.

Note that all powers $\hat{h}_0^k$, $1 \leq k < p$, are also arithmetical. Therefore, we can introduce the appropriate action of the additive group scheme $\text{Spec} \mathbb{F}_p[u]$ and the element $c[u] \in L_{\mathcal{K}} \otimes \mathbb{F}_p$ such that $c[u]|_{u=1} = c$. In addition, $c[u]$ can be uniquely recovered from its “linear term” $c_1 \otimes u = dc[u]$. 
Theorem 4.2. Suppose $\tilde{N} \geq N^*(c_0) - 1$. Then a lift $\tilde{h}_0$ of $h_0$ is arithmetical iff $\operatorname{ad}h_0(L) \subset L^{(c_0)}$ and

$$c_1 \equiv - \sum_{j \in I} \sum_{i=0}^{N^*} \sigma^i(A_j F_{\gamma_i} - \epsilon_{\gamma_i + co} + pj) \mod (L^{(c_0)}_K + \epsilon_{o}(p-1)M_K)$$

Theorem 4.2 will be proved in Subsections 4.3, 4.4 below.

4.4. Auxiliary result. We review here a technical result from [3], Section 3. This result was obtained in the contravariant setting. First we introduce the relevant objects and assumptions.

Introducing objects.

Set $M = 0$ (we need the period $p$ case but all constructions in Section 3 of [3] were done modulo $p^{M+1}$). Let $A = [0, pv_0) \cap \mathbb{Z}^+(p)$, where $v_0 \geq 0$ (later we specify $v_0 = c_0$). Let $L(A)$ be a free Lie algebra over $k = \mathbb{F}_{p^{v_0}}$ with the set of generators

$$\{D\alpha | \alpha \in A^+ = A \cap \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0 \} \cup \{D_0\}$$

For $n \in \mathbb{Z}/N_0$, set $D_{\alpha n} = (\sigma^n \alpha_0)D_0$. Consider the $\sigma$-linear morphism $L(A) \to L(A)$ such that for all $a, n$, $D_{\alpha n} \mapsto D_{\alpha, n+1}$ and denote it also by $\sigma$. Then $L^0 := L(A)|_{\sigma = \text{id}}$ is a free Lie algebra over $\mathbb{F}_p$ and $L^0_k = L(A)$.

Consider the contravariant analogue of the elements $F_{\gamma_i - N}$ from Subsection 1.4 (use the same conditions for all involved indices)

$$F_{\gamma_i - N} = \sum_{1 \leq i < p} (-1)^{s-1} \sum_{n_1 \vdots n_s} a_1[\ldots [D_{a_1 n_1}, D_{a_2 n_2}], \ldots, D_{a_s n_s}]$$

Denote by $L^0_k(v_0)$ the minimal ideal in $L^0$ such that $L^0_k(v_0)_k$ contains all $F_{\gamma_i - N}$, $\gamma \geq v_0$. Let $N^1_0 = N^1_0(v_0, A)$ be such that the ideals $L^0_k(v_0)$ coincide for all $N \geq N^1_0$ and denote this ideal by $L^0(v_0)$.

Let $\Gamma = \Gamma(A, v_0)$ be the set of all $\gamma = a_1 p^{n_1} + \cdots + a_s p^{n_s}$, where all $a_i \in A$, $0 = n_1 \geq n_2 \geq \cdots \geq n_s$, $1 \leq s < p$.

Choosing parameters $\delta, r^*, N^*$:

- let $\delta = \delta(A, v_0) > 0$ be such that $v_0 - \delta > \max\{\gamma | \gamma \in \Gamma, \gamma < v_0\}$ and $v_0 - \delta \in \mathbb{Z}[1/p]$; note that for all $i \geq 1$, we have also

$$v_0 + pi - \delta > \max\{\gamma | \gamma \in \Gamma, \gamma < v_0\}.$$

- let $r^*$ be such that $v_p(r^*) = 0$ and $v_0 - \delta < r^* < v_0$;

- let $N^* \in \mathbb{N}$ be such that $N^* \geq N_1^*$ and for $q = p^{N^*}$, we have $r^*(q - 1) = b^* \in \mathbb{N}$ (note $v_p(b^*) = 0$), $a^* = q(v_0 - \delta) \in p\mathbb{N}$ and $q(b^* - a^*) > pa^*$.

All above constructions and choices were made in Subsection 3.1 of [3]. We need also the following additional restrictions (which obviously do not contradict to the previous ones).
Additional restrictions:

— $p^d < 2v_0$;

— let $e_0^r$ be the ramification index of $\mathcal{K}/\mathcal{K}$; then we assume (by taking sufficiently large $N^*$) that $\varphi_{\mathcal{K}/\mathcal{K}}^{-1}(r^* + q(v_0 - r^*)) > e_0 v_0 (p - 1)$.

We need also the following auxiliary field extension $\mathcal{K}' = \mathcal{K}(r^*, N^*)$ of $\mathcal{K}$ such that:

— $[\mathcal{K}' : \mathcal{K}] = q$;

— the Herbrand function $\varphi_{\mathcal{K}/\mathcal{K}}$ has only one edge point at $(r^*, r^*)$;

— $\mathcal{K}' = k((t_1))$, where $t = t_1^q E(t^p)^{-1}$ with the Artin-Hasse exponential $E(X) = \exp(X + X^p/p + \cdots + X^{p^n}/p^n + \cdots)$.

The field $\mathcal{K}'$ played very important role in our approach to the ramification filtration in $[12345678911]$.

Let $e^{(0)}_L = \sum_{a \in k^0(p)} t^{-a} \mathcal{D}_a$ and $e^{(q)}_L = \sum_{a \in k^0(p)} t_1^{-aq} \mathcal{D}_a$. (We follow maximally close the notation from [3].) Clearly, the elements $e^{(0)}_L$ and $e^{(q)}_L := \sum_{a \in k^0(p)} t^{-a} \mathcal{D}_{a,-N}$ are analogues of the element $e_0$ introduced in Subsection $[1234]$ and $\sigma^N e^{(q)}_L = e^{(q)}_L$.

Let $\widetilde{N} = N^* - 1$ and consider the following element from $G(\mathcal{L}_0)$

$\phi^{(\widetilde{N})}_0 = e^{(q)}_L \circ (\sigma e^{(q)}_L) \circ \cdots \circ (\sigma^N e^{(q)}_L) \circ (-\sigma^N e^{(0)}_L) \circ \cdots \circ (-\sigma e^{(0)}_L) \circ (-e^{(0)}_L)$

Suppose $O = O_{\mathcal{K}'}$ is the valuation ring of $\mathcal{K}'$. Then we have, cf. Proposition from Subsection 3.10 of [3], the following property.

**Proposition 4.3.** a) $\phi^{(\widetilde{N})}_0 \in L^0(v_0)_{\mathcal{K}'} + \sum_{1 \leq j < p} t_1^{-ja^*} C_j(L^0_O)$;

b) $\phi^{(\widetilde{N})}_0 \circ e^{(0)}_L \equiv e^{(q)}_L \circ \sigma \phi^{(\widetilde{N})}_0$ mod $\mathcal{L}_1$, where

$\mathcal{L}_1 = L^0(v_0)_{\mathcal{K}'} + t_1^{q(b - a^*)} \sum_{1 \leq j < p} t_1^{-(j - 1)a^*} C_j(L^0_O)$

Let $v_0 = c_0$.

Consider the map $\Pi$ from $\mathcal{L}_0$ to $\mathcal{L}$ such that $(\Pi \otimes k)(\mathcal{D}_{an}) = \mathcal{D}_{an}$ for all $a \in A$ and $n \in \mathbb{Z}/N_0$ and for any $l_1, l_2 \in \mathcal{L}_0$, $\Pi([l_1, l_2]) = \Pi(l_2), \Pi(l_1)$.

Then the ideal $\mathcal{L}_0(c_0)$ is mapped to $\mathcal{L}(c_0)$. Essentially, $\Pi$ is a morphism of Lie algebras (where $\mathcal{L}_0$ is taken with the opposite Lie structure) and it induces an isomorphism of the appropriate quotients by $\mathcal{L}_0(c_0)$ and $\mathcal{L}(c_0)$, respectively (use that all $D_{an} \in \mathcal{L}_k(c_0)$ if $a > pc_0$).

Clearly, $\Pi(e^{(0)}_L) = e_0$ and $\Pi(e^{(q)}_L) \equiv e_1 := \sum_{a \in k^0(p)} t_1^{-a} \mathcal{D}_{a,-N}$ mod $\mathcal{L}(c_0)$.

Therefore, we have $\Pi(\phi^{(\widetilde{N})}_0) := \phi = (-\phi_0) \circ (\sigma^N \phi_1)$, where $\phi_0 = \sigma^N e_0 \circ \cdots \circ \sigma e_0 \circ e_0$ and $\phi_1 = \sigma^N e_1 \circ \cdots \circ \sigma e_1 \circ e_1$. 

Proposition 4.4. a) \( \phi \in \mathcal{M}_{K'}; \)

b) \( e_0 \circ \phi \equiv \sigma \phi \circ \sigma^{N^*} e_1 \mod \left( \mathcal{L}_{K'}^{(c_0)} + t^{c_0(p-1)} \mathcal{M}_{K'} \right) \)

Proof. Part a) follows from the inequality \( a^* < qc_0 \). For part b) we need for \( 1 \leq j < p, \)

\[ q(b^* - a^*) - (j-1)a^* > (p-j+1)a^* > (p-j-1)qc_0. \]

This follows from the inequality \((p-j+1)a^* > (p-j-1)qc_0\), which can be rewritten as \((p-j+1)(qc_0 - a^*) < 2qc_0\) and is implied by the additional assumption \( p\delta < 2c_0. \)

\[ \square \]

4.5. Action of \( \hat{h}_0 \) on \( \phi_0 \) and \( \phi_1 \). Apply identities \((3.4)\) and \((3.5)\) from Subsection \(3.2\) and use the definition of the elements \( \mathcal{F}_{\gamma,-N}^0 \in \mathcal{L}_k \) from Subsection \(1.4\):

\[
e_0 + d\hat{h}_0^n(e_0) = e_0 \circ \left( \sum_{k \geq 1} \frac{1}{k!} \left[ \ldots [d\hat{h}_0^n(e_0), e_0], \ldots, e_0] \right)_{k-1 \text{ times}} \right)
\]

\[
= e_0 \circ \left( u \sum_{\gamma > 0, j > 0} A_j \mathcal{F}_{\gamma,0}^0 t^{-\gamma + c_0 + pj} \right)
\]

Similarly,

\[
(\sigma e_0 + d\hat{h}_0^n(e_0)) \circ e_0 = (\sigma e_0) \circ \left( u \sum_{\gamma > 0} \sigma(A_j \mathcal{F}_{\gamma,0}^0 t^{c_0 + pj}) \right) \circ e_0
\]

\[
= (\sigma e_0) \circ e_0 \circ \left( u \sum_{k_0 \geq 1} \frac{1}{k_0!} \left[ \ldots [\sigma d\hat{h}_0^0(e_0), \sigma e_0], \ldots, \sigma e_0], e_0], \ldots, e_0] \right)_{k_0-1 \text{ times}} \right)
\]

\[
= (\sigma e_0) \circ e_0 \circ \left( u \sum_{\gamma > 0, j > 0} \sum_{i=0}^1 \sigma^i(A_j \mathcal{F}_{\gamma,-i}^0 t^{-\gamma + c_0 + pj}) \right)
\]

We can continue similarly to obtain that

\[
\hat{h}_0^n(\phi_0) = \phi_0 \circ \left( \sum_{\gamma > 0} \sum_{0 \leq i < N} \sigma^i(A_j \mathcal{F}_{\gamma,-i}^0 t^{-\gamma + c_0 + pj}) \right) \mod u^2
\]

We can treat similarly the action of \( \hat{h}_0^n \) on \( \phi_1 \) but \( \hat{h}_0|_{K'} \in \text{Aut}^{(c')} K' \) with \( c' = \varphi_{K'_{K'}}^{-1}(c_0) = r^* + (c_0 - r^*)q > c_0(p-1), \) cf. Additional restrictions in Subsection \(4.3\). Therefore, \( \hat{h}_0(e_1) \equiv e_1 \mod t^{c_0(p-1)} \mathcal{M}_{K'} \), \( \hat{h}_0(\sigma^{N^*} e_1) \equiv \sigma^{N^*} e_1 \mod t^{c_0(p-1)} \mathcal{M}_{K'} \) and \( \hat{h}_0(\phi_1) \equiv \phi_1 \mod t^{c_0(p-1)} \mathcal{M}_{K'}. \)

Finally, we proved that
Proposition 4.5.

\[
\hat{h}_0(\phi) \equiv \left(-u \sum_{\gamma > 0} \sum_{j \geq 0} \sigma^j(A_j F_{\gamma,j}^0 t_0^{-\gamma+c_0+j})\right) \circ \phi \\
\mod \left(u^2 M_{\mathcal{K}'} + t^{c_0(p-1)} M_{\mathcal{K}'} + L_{\mathcal{K}'}^{(c_0)}\right)
\]

Finish the proof of Theorem 4.2 as follows.
We have \( f_0 = \phi \circ \sigma^{N_s} f_0' \mod t^{c_0(p-1)} M_{\mathcal{K}'} < p \). The field extensions \( \mathcal{K}'_{<p}/\mathcal{K}' \) and \( \mathcal{K}_{<p}/\mathcal{K} \) are isomorphic: an isomorphism of \( \mathcal{K} \) and \( \mathcal{K}' \) which sends \( t \) to \( t' \) (both fields have the same residue field) can be extended to an isomorphism of \( \mathcal{K}_{<p} \) and \( \mathcal{K}'_{<p} \) which sends \( f_0 \) to \( f'_0 \). Therefore, the Herbrand functions of these field extensions coincide and the second additional restriction from Subsection 4.3 implies that \( \hat{h}_0(f'_0) \equiv f'_0 \mod t^{c_0(p-1)} M_{\mathcal{K}_{<p}} \). Therefore,

\[
\hat{h}_0(f_0) \equiv \hat{h}_0(\phi) \circ \sigma^{N_s} f'_0 \mod t^{c_0(p-1)} M_{\mathcal{K}'_{<p}}
\]

and Theorem 4.2 follows from Proposition 4.5.

5. Explicit Form of the Relation in \( L \)

In this Section we apply the above techniques to specify an arithmetical lift \( \hat{h}_0 \) and to find an explicit form of the Demushkin relation in \( L \).

We use all notation from Section 4.

Suppose \( \hat{h}_0 \) is given via \( \hat{h}_0(f_0) = c \circ (Ad \hat{h}_0 \otimes 1) f_0 \) with \( c \in \mathcal{L}_K \). Then the appropriate elements \( c_1 \otimes u = dc[u] \) and \( V_a = ad h_0(D_{a0}) \), \( a \in \mathbb{Z}(p) \), satisfy recurrent relation (4.3). This relation allows us to proceed from \( (c_1, \sum_a t^{-a} V_a) \mod C_s(\mathcal{L}_K) \) to \( (c_1, \sum_a t^{-a} V_a) \mod C_{s+1}(\mathcal{L}_K) \), where \( 1 \leq s < p \). The non-uniqueness of \( \hat{h}_0 \) is related to a non-unique choice of \( c_1 \) on each step.

Let \( c_1 = \sum_{m \in \mathbb{Z}} c_1(m) t^m \), where all \( c_1(m) \in \mathcal{L}_k \). Introduce \( c_1^+ = \sum_{m > 0} c_1(m) t^{-m} \) and \( c_1^- = \sum_{m < 0} c_1(m) t^m \). Then \( c_1 = c_1^- + c_1(0) + c_1^+ \).

In this section we apply Theorem 4.2 to specify the choice of \( c_1 \) such that the appropriate lift \( \hat{h}_0 \) is arithmetical. When choosing \( c_1^+ \) and \( c_1^- \) we can obviously use the operator \( S \) from Subsection 2.2 because \( S(\sigma c_1^+ - c_1^-) = c_1^+ \) and \( S(\sigma c_1^- - c_1^-) = c_1^- \). When choosing \( c_1(0) \) we must act more carefully.

It would be very interesting to resolve recurrent relation (4.3) to get precise explicit formulas for the differentiation \( ad \hat{h}_0 \), where \( \hat{h}_0 \) is arithmetical. This was done below for \( ad \hat{h}_0(D_0) \) and can be stated as the following theorem.
Theorem 5.1. There is an arithmetical lift $\hat{h}_0$ such that
$$\text{ad} \hat{h}_0(D_0) = \sum_{j \geq 0} \text{Tr}_{k/F_p} \left( A_j \mathcal{F}_\sigma^0 \right).$$

Proof of Theorem. Proceed first with explicit formulas for $c_1^+$ and $c_1(0)$.

5.1. Specifying $c_1^+$. Relation (3.3) implies that
$$\sigma c_1^+ - c_1^+ =$$
$$\sum_{k \geq 1} \frac{1}{k!} A_j \sum_{a_1, \ldots, a_k} t^{\sigma (a_1 + \ldots + a_k)} \left[ \ldots [a_1 D_{a_1 0}, D_{a_2 0}], \ldots, D_{a_k 0}] -
\sum_{m, k \geq 1} \frac{1}{k!} \sum_{a_1, \ldots, a_k} t^{\sigma m - (a_1 + \ldots + a_k)} \left[ \ldots \sigma(m), D_{a_1 0}], \ldots, D_{a_k 0}].
$$
In both above sums the indices $a_1, \ldots, a_k$ run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \ldots + a_k < c_0 + pj$ for the first sum and $a_1 + \ldots + a_k < pm$ for the second sum.

Definition. For $n^* \geq n_*$, denote by $\mathcal{F}_{\gamma^*[n^*, n_*]}^0$ the partial sum of $\sigma^n \mathcal{F}_{\gamma^*-n^*}^0$ containing only the terms with $\ldots [D_{a_1 n_1}, D_{a_2 n_2}], \ldots, D_{a_* n_*}]$, where $n_1 = n^*$ and $n_* = n_*$. In other words, we keep only the terms such that $n^* = \max\{n_i \mid 1 \leq i \leq s\}$ and $n_* = \min\{n_i \mid 1 \leq i \leq s\}$.

Lemma 5.2. There is an arithmetical lift $\hat{h}_0$ of $h_0$ such that:

a) the right-hand side of (5.1) is congruent to
$$\sum_{j \geq 0} \sigma^n(A_j) \sum_{0 \leq n < n^*} \mathcal{F}_{\gamma^*[n, 0]}^0 t^{\sigma (n^* - n)} \mod t^{\sigma(p-1)} \mathcal{L}_{O_K};$$

b) $c_1^+ \equiv -\sum_{j \geq 0} \sum_{0 \leq n < n^*} \sigma^n(A_j) \mathcal{F}_{\gamma^*-n}^0 t^{\sigma(n^* - n)} \mod t^{\sigma(p-1)} \mathcal{L}_{O_K}.$

Proof of Lemma. It will be sufficient to prove the existence of a lift $\hat{h}_0$ such that recurrent relation (3.3) is satisfied with the right-hand side and the part $c_1^+$ of $c_1$ from parts a) and b) of our lemma. (Use that the part $c_1^+$ of $c_1$ satisfies the criterion from Theorem 4.2.)

To prove that the congruences a) and b) are satisfied modulo all $C_s(L_K)$, $1 \leq s \leq p$, by induction on $s$ if we agree to recover the part $c_1^+$ of $c_1$ in (3.3) via the operator $S$ from Subsection 2.2.

Prove that b) modulo $C_s(L_K)$ implies a) modulo $C_{s+1}(L_K)$.

Note that for $n = 0$,
$$\mathcal{F}_{\gamma^*[0, 0]}^0 = \sum_{a_1, \ldots, a_k} \frac{1}{k!} \left[ \ldots [a_1 D_{a_1 0}, D_{a_2 0}], \ldots, D_{a_k 0}.$$
and for $n > 0$,

$$
\mathcal{F}^0_{\gamma,[n,0]} = \sum_{k \geq 1, \gamma > 0, a_1, \ldots, a_k} \frac{1}{k!} \left[ \ldots [\sigma^n \mathcal{F}^0_{\gamma,-(n-1)}, D_{a_10}], \ldots, D_{a_k0}] \right].
$$

In both sums the indices $a_1, \ldots, a_k$ run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \cdots + a_k = \gamma$ in the first case and $p^n \gamma' + a_1 + \cdots + a_k = \gamma$ in the second case.

The first formula allows us to identify the second line in (5.1) with the part of a) which corresponds to $n = 0$. The second formula allows us to rewrite modulo $C_{s+1}(L_K)$ the third line in (5.1) as the part of a) which corresponds to $n > 0$.

Prove that a) modulo $C_s(L_K)$ implies b) modulo $C_s(L_K)$.

Let $\Omega$ be the right-hand side of (5.1). Applying $S$ we obtain

$$
c_1^+ \equiv - \sum_{n,m,j} \sigma^{n+m} \left( A_j \mathcal{F}^0_{\gamma,[0,-n]} \right) t^{p^{n+m}(c_0+pj-\gamma)} \mod t^{c_0(p-1)}L_K + C_s(L_K).
$$

Modulo $t^{c_0(p-1)}$ we can assume that $n_1 = n + m < N^*$ and rewrite the above right-hand side as

$$
- \sum_{\gamma, j, n_1} \sigma^{n_1} \left( A_j \sum_{0 \leq m \leq n_1} \mathcal{F}^0_{\gamma,[0,-m]} \right) t^{p^{n_1}(c_0+pj-\gamma)}.
$$

It remains to note that $\sum_{0 \leq m \leq n_1} \mathcal{F}^0_{\gamma,[0,-m]} = \mathcal{F}^0_{\gamma,-n_1}$. \qed

5.2. Specifying $c_1(0)$. By (3.3) we have

$$(5.2) \quad \sigma c_1(0) - c_1(0) + V_0 =$$

$$
\sum_{k \geq 1} \sum_{a_1, \ldots, a_k} \frac{1}{k!} A_j \left[ \ldots [a_1D_{a_10}, D_{a_20}], \ldots, D_{a_k0}] \right] -
$$

$$
\sum_{k,n \geq 1} \frac{1}{k!} \left[ \ldots [\sigma c_1^+(m), D_{a_10}], \ldots, D_{a_k0}] \right] -
$$

$$
\sum_{k \geq 2} \frac{1}{k!} \left[ \ldots [V_0, D_{00}], \ldots, D_{00}] \right] \underset{k-1 \text{ times}}{\underbrace{\ldots \ldots \ldots \ldots \ldots \ldots}} -
$$

$$
\sum_{k \geq 1} \frac{1}{k!} \left[ \ldots [\sigma c_1(0), D_{00}], \ldots, D_{00}] \right] \underset{k \text{ times}}{\underbrace{\ldots \ldots \ldots \ldots \ldots \ldots}}
$$

In the first and second sums the indices $a_i$ run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \cdots + a_k = c_0 + pj$ in the first case and $a_1 + \cdots + a_k = pm$ in the second case.
**Definition.** For \( n \geq 0 \), denote by \( F^+_{\gamma,[n,0]} \) the partial sum of \( F^0_{\gamma,[n,0]} \) which contains only the terms with \([\ldots, D_{a_1n_1}, D_{a_2n_2}, \ldots, D_{a_in_i} \ldots] \) such that if for some \( i_1 \geq 0 \), \( 0 = n_s = \cdots = n_{s-i_1} < n_{s-i_1-1} \) then at least one of \( a_s, \ldots, a_{s-i_1} \) is not zero.

The following lemma follows directly from the above definition.

**Lemma 5.3.** In the right-hand side of \((5.2)\) the sum of the first two sums equals

\[
\sum_{0 \leq n < N^*} \sigma^n(A_j) F^+_{\gamma,[n,0]}
\]

5.3. **Operators** \( F_0 \) and \( G_0 \). For \( i \in \mathbb{Z}/N_0 \), introduce the operators

\[
G_i = \exp(-adD_0i), \quad F_i = X^{-1}(1 - \exp(-X))|_{X = adD_0i}
\]

on \( L_k \). Note that for \( l \in L_k \),

\[
F_i(l) = \sum_{k \geq 1} \frac{1}{k!} \ldots \left[ l, \underbrace{D_0, \ldots, D_0} \right]_{k-1 \text{ times}} \quad G_i(l) = \sum_{k \geq 0} \frac{1}{k!} \ldots \left[ l, \underbrace{D_0, \ldots, D_0} \right]_{k \text{ times}}
\]

With this notation we can rewrite \((5.2)\) in the following form

\[
(G_0 - \text{id})c_1(0) + F_0(V_0) = \sum_{j \geq 0} \sum_{0 \leq n < N^*} \sigma^n(A_j) F^+_{\gamma,[n,0]}
\]

**Lemma 5.4.** Suppose \( l(\alpha, \gamma) = \sum_{0 \leq i < N^*} \sigma^i(\alpha F^0_{\gamma,-i}) \), where \( \alpha \in k \). Then

\[
(G_0 - \text{id})l(\alpha, \gamma) = - \sum_{0 \leq i < N^*} \sigma^i(\alpha F^0_{\gamma,-i}) + \sigma^{N^*}(\alpha F^0_{\gamma,-N^*})
\]

**Proof of Lemma.** First, directly from definitions it follows for \( i \geq 0 \), that

\[
\sigma^i F^0_{\gamma,-i} = \sum_{0 \leq s \leq i} (G_0\sigma)^s F^0_{\gamma,[i-s,0]}
\]

Therefore,

\[
(G_0\sigma)l(\alpha, \gamma) = \sum_{0 \leq s \leq i < N^*} (G_0\sigma)^{s+1} \left( \sigma^{i-s}(\alpha F^0_{\gamma,[i-s,0]} \right) =
\]

\[
\sum_{1 \leq s \leq i < N^*} (G_0\sigma)^s \left( \sigma^{i-s}(\alpha F^0_{\gamma,[i-s,0]} \right) =
\]

\[
\sum_{1 \leq i < N^*} \sigma^i(\alpha F^0_{\gamma,-i}) - \sum_{1 \leq i < N^*} \sigma^i(\alpha F^0_{\gamma,[i,0]} =
\]

\[
l(\alpha, \gamma) - \sum_{0 \leq i < N^*} \sigma^i(\alpha F^0_{\gamma,[i,0]} + \sigma^{N^*}(\alpha F^0_{\gamma,-N^*})
\]

□
Corollary 5.5. a) For $c'_1(0) = c_1(0) + \sum_{0 \leq i < N, j \geq 0} \sigma^j(A_j F^0_{c + pj, -j})$ relation (5.2) can be rewritten as

$$(G_0 \sigma - \text{id})c'_1(0) + F_0(V_0) = \sum_{j \geq 0} \sigma^{N^*} (A_j F^0_{c + pj, -N^*});$$

b) the lift $\hat{h}_0$ is arithmetical if $c'_1(0) \in L^{(co)}_k$ (and $V_0 \in \alpha_0 L^{(co)}$).

Proof of Corollary. Apply Lemma 5.4 and note that for any $j \geq 0$, $F^+_0(c + pj, [N^*]) = 0$. □

5.4. The end of proof of Theorem 5.1. All we need now is the following proposition.

Proposition 5.6. For $\omega \in L^{(co)}_k$, there are $x_0 \in L^{(co)}_k$ and $y_0 \in \alpha_0 L^{(co)}$ such that $y_0 \equiv \alpha_0 \text{Tr}_{K/F_p}(\omega) \mod \alpha_0[D_0, L^{(co)}]$ and

$$(G_0 \sigma - \text{id})x_0 + F_0(y_0) = \omega$$

Proof. The proof is obtained by induction on $s$ modulo the descending series of ideals $\text{ad}^s(D_{00})(L^{(co)}_k)$, $s = 1, \ldots, p - 1$. □

Theorem 5.1 is completely proved. □

6. Applications to the mixed characteristic case

Let $K$ be a finite field extension of $\mathbb{Q}_p$ with the residue field $k \cong \mathbb{F}_p^{\pi_0}$ and the ramification index $e$. Let $\pi_0$ be a uniformising element in $K$. Denote by $\bar{K}$ an algebraic closure of $K$ and set $\Gamma_K = \text{Gal}(\bar{K}/K)$. Assume that $K$ contains a primitive $p$-th root of unity $\zeta_1$.

6.1. For $n \in \mathbb{N}$, choose $\pi_N \in \bar{K}$ such that $\pi_n^p = \pi_{n-1}$. Let $\bar{K} = \bigcup_{n \in \mathbb{N}} K(\pi_n)$, $\Gamma_K(1) := \Gamma_K/\Gamma_K^p C_p(\Gamma_K)$ and $\Gamma_{\bar{K}} = \text{Gal}(\bar{K}/\bar{K})$. Then a natural embedding $\Gamma_{\bar{K}} \subset \Gamma_K$ induces a continuous group homomorphism $i : \Gamma_{\bar{K}} \rightarrow \Gamma_K(1)$.

We have $\text{Gal}(K(\pi_1)/K) = \langle \tau_0 \rangle^{Z/p}$, where $\tau_0(\pi_1) = \pi_1 \zeta_1$. Let $j : \Gamma_K(1) \rightarrow \text{Gal}(K(\pi_1)/K)$ be a natural epimorphism.

Proposition 6.1. The following sequence

$$\Gamma_{\bar{K}} \xrightarrow{i} \Gamma_K(1) \xrightarrow{j} \langle \tau_0 \rangle^{Z/p} \rightarrow 1$$

is exact.

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

Consider $\bar{K}^\prime = \bigcup_{n \in \mathbb{N}} K(\pi_n, \zeta_n)$. Then $\bar{K}^\prime/K$ is Galois with the Galois group $\Gamma_{\bar{K}^\prime/K} = \langle \sigma, \tau \rangle$. Here for any $n \in \mathbb{N}$ and some $s_0 \in p\mathbb{Z}$, $\sigma \zeta_n = \zeta_n^{1+p s_0}$, $\sigma \pi_n = \pi_n$, $\tau(\zeta_n) = \zeta_n$, $\tau \pi_n = \pi_n \zeta_n$ and $\sigma^{-1} \tau = \tau(1+p s_0)^{-1}$. 
Therefore, $C_2(\tilde{\Gamma}/K) = \langle \tau^p \rangle \subset \tilde{\Gamma}/K$, $\tilde{\Gamma}/K \overset{\sigma}{\to} \tilde{\Gamma}/K$, and we have a natural exact sequence

$$\langle \sigma \rangle \rightarrow \tilde{\Gamma}/K(1) \rightarrow \langle \tau \rangle \quad \text{mod} \langle \tau^p \rangle = \langle \tau_0 \rangle^{Z/p} \rightarrow 1.$$ 

Note that $\tilde{\Gamma}$, together with a lift $\tilde{\sigma} \in \tilde{\Gamma}$ of $\sigma$ generate $\tilde{\Gamma}$.

The above short exact sequence implies that $\text{Ker}(\tilde{\Gamma}(1) \rightarrow \langle \tau_0 \rangle^{Z/p})$ is generated by $\tilde{\sigma}$ and the image of $\tilde{\Gamma}$. So, the kernel coincides with the image of $\tilde{\Gamma}$ in $\Gamma(1)$. \hfill $\square$

6.2. Let $R$ be Fontaine’s ring. We have a natural embedding $k \subset R$ and an element $t = (\pi_\alpha \text{ mod } p)_{\alpha \geq 0} \in R$. If $K = k((t))$ and $R_0 = \text{Frac } R$ then $K$ is a closed subfield of $R_0$ and the theory of the field-of-norms functor \cite{30} identifies $R_0$ with the completion of the separable closure $K_{\text{sep}}$ of $K$ in $R_0$.

This allows us to identify $\Gamma_K = \text{Gal}(K_{\text{sep}}/K)$ with $\tilde{\Gamma} \subset \Gamma_K$. Let $\Gamma_K(1) = \Gamma_K/\tilde{\Gamma}\tau(C_\Gamma)$. Note that we have a natural continuous epimorphism $\iota$ of the infinite group $\Gamma_K(1)$ to the finite group $\Gamma_K(1)$. Therefore, we obtain the following property.

**Proposition 6.2.** The following natural short exact sequence

$$\Gamma_K(1) \rightarrow \tilde{\Gamma}(1) \rightarrow \langle \tau_0 \rangle^{Z/p} \rightarrow 1$$

is exact.

6.3. Let $v_K$ be the extension of the normalised valuation on $K$ to $R_0$.

Consider a closed field isomorphism $\eta : K \rightarrow R_0$ compatible with $v_K$. Denote by $\text{Iso}(\eta, K_{<p}, R_0)$ the set of all extensions of $\eta$ to $K_{<p}$. This set is a principal homogeneous space over $\Gamma_K/\tilde{\Gamma} = G(L)$.

We can specify each $\tilde{\eta} \in \text{Iso}(\eta, K_{<p}, R_0)$ by choosing $f_0' = \tilde{\eta}(f_0) \in L_{R_0}$ such that $\sigma f_0' = e_0 \circ f_0'$. (The elements $e_0 \in L_K$ and $f_0 \in L_{K_{\text{sep}}}$ were chosen in Subsection \cite{13})

Let $c_0 := ep/(p - 1)$. Consider the appropriate submodules $M_K \subset L_K$, $M_{K_{\text{sep}}} \subset L_{K_{\text{sep}}}$ and define similarly $M_{R_0} \subset L_{R_0}$, cf. Subsection \cite{23}. We know that $\sigma f_0 \in M_K$, $f_0 \in M_{K_{\text{sep}}}$ and for similar reasons, $f_0' \in M_{R_0}$.

**Lemma 6.3.** Suppose $\eta$ is such that $\eta(e_0) \equiv e_0 \mod t^{(p-1)c_0} M_{R_0}$. then there is $c \in t^{(p-1)c_0} M_{R_0}$ such that $\eta(e_0) = c \sigma c - e_0 \circ (\sigma c) - c$.

**Proof.** Note that $t^{(p-1)c_0} M_{R_0}$ is an ideal in $M_{R_0}$ and for any $i \in \mathbb{N}$ and $m \in t^{(p-1)c_0} C_i(M_{R_0})$, we can always find $c \in t^{(p-1)c_0} C_i(M_{R_0})$ such that $\sigma c - c = m$.

Therefore, there is $c_1 \in t^{(p-1)c_0} M_{R_0}$ such that $\eta(e_0) = e_0 + \sigma c_1 - c_1$. This implies that $\eta(e_0) \circ c_1 \equiv \sigma c_1 \circ e_0 = \langle \tau_0 \rangle^{Z/p} \mod t^{(p-1)c_0} C_2(M_{R_0})$. Similarly, there is $c_2 \in t^{(p-1)c_0} C_2(M_{R_0})$ such that $\eta(e_0) \circ c_1 + c_2 = \sigma c_2 + \sigma c_1 \circ e_0$ and $\eta(e_0) \circ c_1 \circ c_2 \equiv \sigma c_2 \circ \sigma c_1 \circ e_0 \mod t^{(p-1)c_0} C_3(M_{R_0})$. 

After \( p - 1 \) iterations we obtain for \( 1 \leq i < p \) the elements \( c_i \in t^{(p - 1)i}C_t(M_{R_0}) \) such that
\[
\eta(e_0) \circ (c_1 \circ \cdots \circ c_{p-1}) = \sigma(c_{p-1} \circ \cdots \circ c_1) \circ e_0.
\]
The lemma is proved. \( \square \)

The above lemma implies the following properties:

**Proposition 6.4.** a) If \( \eta(e_0) \equiv e_0 \mod t^{(p - 1)c_0}M_{R_0} \) then for any \( \tilde{\eta} \in \text{Iso}(\eta, K_{<p}, R_0) \), there is a unique \( c \in G(L) \) such that
\[
\tilde{\eta}(f_0) = f_0 \circ c \mod t^{(p - 1)c_0}M_{R_0};
\]

b) Suppose the field embeddings \( \eta_1, \eta_2 : K \to R_0 \) are such that \( \eta_1(t) \equiv \eta_2(t) \mod t^{(p - 1)c_0}m_R \). Then for any \( \tilde{\eta}_1 \in \text{Iso}(\eta_1, K_{<p}, R_0) \), there is a unique \( \tilde{\eta}_2 \in \text{Iso}(\eta_2, K_{<p}, R_0) \) such that
\[
\eta_1(f_0) \equiv \eta_2(f_0) \mod t^{(p - 1)c_0}M_{R_0}.
\]

6.4. Let \( \varepsilon = (\zeta_n \mod p)_{n \geq 0} \in R \) be Fontaine’s element (here \( \zeta_0 = 1 \) and the others \( \zeta_n \) were introduced in Subsection 6.1).

Let \( \zeta_i = 1 + \sum_{i \geq 1} \beta_i \pi_0^i \) with all \( \beta_i \in k \). Use the rings identification \( R/t^{pe_K} \simeq O_K/p \), coming from the natural projection \( R \to (O_K/p)_1 \). This implies that
\[
\varepsilon \equiv 1 + \sum_{i \geq 1} \alpha_i t^i \mod t^{pe_K}
\]
where \( \alpha_i \in k \), \( \alpha_i = 0 \) if \( i \neq 0 \mod p \), \( \alpha_{pi} = \beta_i^p \) and \( \alpha_i = 0 \) if \( i < c_0 := pe/(p - 1) \).

Let \( h_0 \in \text{Aut}K \) be such that \( h_0 |_{k} = \text{id} \) and \( h(t) = t(1 + \sum_{i \geq 1} \alpha_i t^i) \).

Clearly, \( h_0(t) \equiv \tau_0(t) \mod t^{(p - 1)c_0}M_{R_0} \). The proposition 6.4b) implies that the orbits of \( f_0 \mod t^{(p - 1)c_0}M_{R_0} \) with respect to the action of \( \Gamma_K \) and \( \tilde{G}_{h_0} \) coincide. Therefore, we have a natural isomorphism \( \tilde{G}_{h_0} \to \Gamma_K(1) \). In addition, this isomorphism is compatible with the ramification filtration on these groups. (Use that the ramification filtrations coincide on \( L/L(p) \) and the appropriate lifts \( \tilde{h}_0 \) and \( \tilde{\tau}_0 \) are both arithmetical, because the Criterion from Theorem 4.2 takes into account the behaviour of \( \tilde{h}_0 \) modulo \( t^{(p - 1)c_0}M_{R_0} \).

As a result we have the following construction of the Galois group \( \Gamma_K(1) \) together with its ramification filtration \( \{ \Gamma_K(1)_n \}_{n \geq 0} \).

**Group structure:**

\( \Gamma_K(1) = G(L) \), where \( L \) is the Lie \( \mathbb{F}_p \)-algebra such that
\[
0 \to L/L(p) \to L \to \mathbb{F}_p\pi_0 \to 0.
\]

— the Lie algebra \( L \) was defined in Subsection 1.3.

— \( L \) has standard system of generators
\[
\{ D_n \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0 \} \cup \{ D_0 \}
\]
— the ideals $\mathcal{L}(s)$, $2 \leq s \leq p$, are given by Theorem (2.3);
— the structure of $L$ is determined by a lift $\hat{\tau}_0$ of $\tau_0$ and the appropriate differentiation $ad\hat{\tau}_0$ described via recurrent relation (3.3);
— for $2 \leq s < p$, $C_s(L) = \mathcal{L}(s)/\mathcal{L}(p)$;

**Ramification filtration:**
— if $K_{s+1} := K_{<p+1}^{C_s}$ then the maximal upper ramification number for $K_{s+1}$ is $c_0$ if $s = 1$ and $c_0 + (c_0(s - 1) - 1)/p$ if $2 \leq s < p$ (use the estimate from Subsection (2.5) and the Herbrand function $\varphi_K(\pi_1/K)$);
— $\hat{\tau}_0$ is arithmetical, i.e. $\hat{\tau}_0 \in L^{(c_0)}$, if the appropriate solutions $c_1$ and $\{V_a \mid a \in \mathbb{Z}^0(p)\}$ of (3.3) are chosen as it is indicated in Section 5;
— if $v \leq c_0$ and $\hat{\tau}_0$ is arithmetical then $\Gamma_K(1)^{(v)}$ is the subgroup of $\Gamma_K(1)$ generated by the image of $G(L^{(v)})$ and $\hat{\tau}_0$;
— if $v > c_0$ then $\Gamma_K(1)^{(v)}$ is the image of $G(L^{(v^*)})$, where $v^* = c_0 + p(v - c_0)$ (use the Herbrand function for $K(\pi_1)/K$);
— if $\hat{\tau}_0$ is arithmetical then the Demushkin relation for $L$, i.e. the element $ad\hat{\tau}_0(D_0) \in \mathcal{L}$, is given by Theorem (5.1).

**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. A. Abrashkin *A group-theoretical property of the ramification filtration*, Izvestiya RAN: Ser. Mat., 62, no.6 (1998), 3-26; English transl. Izvestiya: Mathematics 62, no.6 (1998), 1073–1094
[5] V. Abrashkin, *Report on the ramification filtration of the Galois group of a local field*, Proceedings of the Research Conference on “Number Theory and Arithmetical Geometry: Arithmetical applications of Modular Forms” (San Feliu de Guixols, Spain, 24-29 October, 1997) Inst. fur Exp. Math. Universitat Essen, 1998, 47-53
[6] V. Abrashkin, *On a local analogue of the Grothendieck Conjecture*, Int. J. Math. (2000) 11, no.1, 3–43
[7] V. Abrashkin, *Ramification theory for higher dimensional fields*, Contemp. Math. (2002) 300, 1-16
[8] V. Abrashkin, *Characteristic p case of the Grothendieck conjecture for 2-dimensional local fields*, Proceedings of Steklov Institute (2003) 241, 1-35
[9] V. Abrashkin, *Characteristic p analogue of modules with finite crystalline height*, Pure Appl. Math. Q., 5 (2009), 469–494
[10] V. Abrashkin, *Modified proof of a local analogue of the Grothendieck Conjecture*. Journal Théorie des Nombres de Bordeaux 22, (2010), 1-50
[11] V. Abrashkin, *Galois groups of local fields, Lie algebras and ramification*, 2014, 21 pages
AUTOMORPHISMS OF PERIOD $p$ AND NILPOTENT CLASS $< p$

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

[13] A. Bonfiglioli, R. Fulci, *Topics in Noncommutative Algebra*, Lecture Notes in Mathematics 2034, Springer-Verlag Berlin heidelberg 2012

[14] P. Deligne, *Les corps locaux de caractéristique $p$, limites de corps locaux de caractéristique 0*, Representations of reductive groups over a local field, Travaux en cours, Hermann, Paris, 1973, 119-157

[15] N. L. Gordeev, *Ramification groups of infinite $p$-extensions of a local field*, Soviet Math. 20, no. 6 (1982)

[16] N. L. Gordeev, Infinity of the number of relations in the Galois group of the maximal $p$-extension of a local field with bounded ramification, Izvestia AN SSSR, Ser. Matem. (1981) 45, 592-607

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

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

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

[20] H. Koch, E. de Shalit, *Metabelian local class field theory*, J. Reine Angew. Math. (1996) 478, 85-106

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

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

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

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

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

[26] J.-P. Serre, *Cohomologie Galoisiene*, Springer Verlag, Berlin-Göttingen-Heidelberg-New York, 1964

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

[28] I. R. Shafarevich, *On $p$-extensions (In Russian)*, Mat. Sbornik (1947) 20, 351-363

[29] 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

[30] J.-P. Wintenberger, *Extensions de Lie et groupes d'automorphismes des corps locaux de caractéristique $p$*. (French) C. R. Acad. Sci. Paris Sér. A-B 288 (1979), no. 9, A477-A479

[31] W. Zink, *Ramification in local Galois groups; the second central step*, Pure Appl. Math. Q. 5 (2009), no. 1, 295338.