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

VICTOR ABRASHKIN

ABSTRACT. Suppose K is a finite field extension of $\mathbb{Q}_p$ containing a primitive p-th root of unity. Let $\Gamma_{<p}$ be the maximal quotient of period p and nilpotent class $< p$ of the Galois group of a maximal p-extension of K. We describe the ramification filtration $\{\Gamma^{(v)}_{<p}\}_{v\geqslant 0}$ and relate it to an explicit form of the Demushkin relation for $\Gamma_{<p}$. The results are given in terms of Lie algebras attached to the appropriate p-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, $p > 2$.

In this paper we continue to study the arithmetical structure of the Galois group of complete discrete valuation fields of mixed characteristic initiated in [6].

Let K be a complete discrete valuation field of characteristic 0 with residue field $k \simeq \mathbb{F}_{p^{N_0}}$, $N_0 \in \mathbb{N}$. Set $\Gamma = \mathrm{Gal}(\bar{K}/K)$ and $\Gamma_{<p} = \Gamma/\Gamma^p C_p(\Gamma)$, where $C_p(\Gamma)$ is the subgroup of p-th commutators in Γ. We use equivalence of the categories of p-groups and nilpotent $\mathbb{Z}_p$-algebras Lie of nilpotent class $< p$: the group $\Gamma_{<p}$ is isomorphic to the group $G(L)$, where L is a Lie $\mathbb{F}_p$-algebra of nilpotent class $< p$ and the set $G(L) := L$ is provided with the Campbell-Hausdorff composition law $\circ$ (for any $l_1, l_2 \in L$, $l_1 \circ l_2 = \log(\exp(l_1)\exp(l_2))$.

Assume that K contains a primitive p-th root of unity ζ_1. Let e_K be the ramification index of K and set $c_0 = e^* = e_K p/(p-1) \in p\mathbb{N}$. We use the notation c_0 (resp., e^*) when working with fields of characteristic p (resp., 0). Recall briefly the main results from [6]. (For two R-modules A and S we usually write A_S instead of $A \otimes_R S$.)

a) *Relation to the characteristic p case.*

Fix a uniformizer π_0 in K and let $\widetilde{K} = K(\{\pi_n \mid n \in \mathbb{N}\})$, where $\pi_n^p = \pi_{n-1}$. Then the field-of-norms functor X provides us with a complete discrete valuation field $X(\widetilde{K}) = \mathcal{K}$ of characteristic p with residue field k and fixed uniformizer $t = \varprojlim \pi_n$. There is also a natural identification of $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$ with $\Gamma_{\widetilde{K}} = \mathrm{Gal}(\bar{K}/\widetilde{K})$. This gives

2010 *Mathematics Subject Classification.* 11S15, 11S20.

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

us the exact sequence of p-groups (where $\mathcal{G}_{<p}$ is an analog of $\Gamma_{<p}$ and $\tau_0\in\mathrm{Gal}(K(\pi_1)/K)$ is such that $\tau_0(\pi_1)=\zeta_1\pi_1$)

$$\mathcal{G}_{<p}\xrightarrow{\iota_{<p}}\Gamma_{<p}\longrightarrow\langle\tau_0\rangle^{\mathbb{Z}/p}\longrightarrow 1\,. \tag{0.1}$$

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 algebra over $\mathbb{F}_p$, which depends on the uniformizer $t\in\mathcal{K}$ and a choice of $\alpha_0\in k$ such that $\mathrm{Tr}_{k/\mathbb{F}_p}(\alpha_0)=1$. The algebra $\mathcal{L}_k$ has a system of generators $\{D_{an}\mid a\in\mathbb{Z}^+(p), n\in\mathbb{Z}/N_0\}\cup\{D_0\}$, where $\mathbb{Z}^+(p)=\{a\in\mathbb{N}\mid \gcd(a,p)=1\}$. Note that for all a and n, $\sigma(D_{an})=D_{a,n+1}$ where σ is the morphism of p-th power. With this notation, let $e=\sum_{a\in\mathbb{Z}^+(p)}t^{-a}D_{a0}+\alpha_0D_0\in\mathcal{L}_{\mathcal{K}}$, fix a choice of $f\in\mathcal{L}_{\mathcal{K}_{sep}}$ such that $\sigma f=e\circ f$ and set for any $\tau\in\mathcal{G}_{<p}$,

$$\eta_0(\tau)=(-f)\circ\tau(f)\in G(\mathcal{L})\,.$$

We treat D_0 in the context of others D_{an} by setting $D_{0n}:=\sigma^n(\alpha_0)D_0$.

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

With respect to the identification η_0, the images $\mathcal{G}^{(v)}_{<p}$ of the ramification subgroups $\mathcal{G}^{(v)}\subset\mathcal{G}$ in $\mathcal{G}_{<p}$ come from ideals $\mathcal{L}^{(v)}$ of $\mathcal{L}$. For all $\gamma\in\mathbb{Q}_{>0}$ and $N\in\mathbb{Z}$, there are explicitly defined $\mathcal{F}^0_{\gamma,-N}\in\mathcal{L}_k$, cf. Section 1.4 of [6], such that for any $v\geqslant 0$ and sufficiently large (fixed) $N\geqslant\widetilde{N}(v)$, $\mathcal{L}^{(v)}$ appears as the minimal ideal in $\mathcal{L}$ such that $\mathcal{F}^0_{\gamma,-N}\in\mathcal{L}^{(v)}_k$ for all $\gamma\geqslant v$.

d) *Fundamental sequence of Lie algebras.*

Use equivalence of the categories of p-groups and Lie algebras of nilpotent class $<p$ to replace (0.1) by the exact sequence of Lie $\mathbb{F}_p$-algebras $\mathcal{L}\xrightarrow{\iota_{<p}}L\longrightarrow\mathbb{F}_p\tau_0\longrightarrow 0$. Let $\{\mathcal{L}(s)\}_{s\geqslant 1}$ be the minimal central filtration of ideals in $\mathcal{L}$ such that for all s, $D_{an}\in\mathcal{L}(s)_k$ if $a\geqslant(s-1)c_0$. Then $\mathrm{Ker}\,\iota_{<p}=\mathcal{L}(p)$ and we obtain the exact sequence of Lie $\mathbb{F}_p$-algebras with $\bar{\mathcal{L}}=\mathcal{L}/\mathcal{L}(p)$

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

e) *Replacing τ_0 by $h\in\mathrm{Aut}\mathcal{K}$.*

When studying the structure of (0.2) we can replace τ_0 by a suitable $h\in\mathrm{Aut}\mathcal{K}$. This allows us to apply formalism of nilpotent Artin-Schreier theory to specify a lift $\tau_{<p}$ of τ_0 to L and to introduce a recurrent procedure of recovering $\mathrm{ad}\,\tau_{<p}(D_{an}):=[D_{an},\tau_{<p}]\in\bar{\mathcal{L}}_k$ and $\mathrm{ad}\,\tau_{<p}(D_0):=[D_0,\tau_{<p}]\in\bar{\mathcal{L}}$. More precisely, suppose

$$\zeta_1\equiv 1+\sum_{i\geqslant 0}[\beta_i]\pi_0^{(c_0/p)+i}\,\mathrm{mod}\,p$$

with Teichmüller representatives $[\beta_i]$ of $\beta_i \in k$. Then h can be defined as follows: $h|_k = \mathrm{id}_k$ and $h(t) = t(1+\sum_{i\geqslant 0}\beta_i^p t^{c_0+pi}) = t\widetilde{\exp}(\omega(t)^p)$, where $\widetilde{\exp}$ is the truncated exponential and $\omega(t) \in t^{c_0/p}k[[t]]^*$.

f) *The structure of* L.

Analyzing the above recurrent procedure modulo $C_2(\bar{\mathcal{L}})_k$ we obtained that the knowledge of the elements $\mathrm{ad}\tau_{<p}(D_{an})$ allows us to kill all generators D_{an} of $\bar{\mathcal{L}}_k$ with $a > e^*$. 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, $\mathrm{ad}\tau_{<p}(D_0) \in C_2(\bar{\mathcal{L}}) \subset C_2(L)$ appears as (the Demushkin) relation for L.

In this paper we study the ramification ideals $L^{(v)}$ of L, i.e. the ideals such that $\Gamma^{(v)}_{<p} = G(L^{(v)})$, where $\Gamma^{(v)}_{<p}$ are the images of $\Gamma^{(v)} \subset \Gamma$ in $\Gamma_{<p}$. These steps could be briefly outlined as follows.

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

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 $\varphi_{\widetilde{K}/K}$. This allows us to find 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 $\leqslant s$. The ramification ideals $L^{(v)}$ with $v \leqslant e^*$ require an additional generator – a "good" lift $\tau_{<p}$ of τ_0 (i.e. such that $\tau_{<p} \in L^{(e^*)}$). A characterization of such lifts is the most difficult part of the paper where we need a technical result from [3].

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

The formulas for $\mathrm{ad}\tau_{<p}(D_{an})$ and $\mathrm{ad}\tau_{<p}(D_0)$ have been obtained modulo $C_3(L_k)$ as a second central step of our recurrent procedure in [6], Subsection 3.6. A general expression for $\mathrm{ad}\tau_{<p}(D_0)$ is given in Section 3 – this is explicit form of the Demushkin relation in terms of ramification generators $\mathcal{F}^0_{\gamma,-N}$.

Remark. The numbers $v[s]$, $2 \leqslant s < p$, were found in [5] in a more general context of p-extensions with Galois groups of nilpotent class $< p$ and period p^M, $M \in \mathbb{N}$, but the proof contains a gap. In Section 4 we gave a corrected version in the case $M = 1$; the same procedure can be applied in the case of arbitrary M.

0.1. **Main results.** Suppose for all $a \in \mathbb{Z}^0(p) := \mathbb{Z}^+(p) \cup \{0\}$, $V_{a0} \in \bar{\mathcal{L}}_k$ are such that $\mathrm{ad}\tau_{<p}(D_{a0}) = V_{a0}$. In particular, $V_{00} = \alpha_0 V_0$, where $V_0 = (\mathrm{ad}\tau_{<p})D_0 \in \bar{\mathcal{L}}$, and the knowledge of all V_{a0} determines uniquely the differentiation $\mathrm{ad}\tau_{<p}$ (note that for all n, $\mathrm{ad}\tau_{<p}(D_{an}) = \sigma^n(V_{a0})$).

The recurrent relation from [6] appears in the following form

$$\sigma c_1 - c_1 + \sum_{a\in\mathbb{Z}^0(p)} t^{-a} V_{a0} = \tag{0.3}$$

$$-\sum_{k\geqslant 1}\frac{1}{k!}\,t^{-(a_1+\dots+a_k)}\omega(t)^p[\dots[a_1D_{a_10},D_{a_20}],\dots,D_{a_k0}]$$
$$-\sum_{k\geqslant 2}\frac{1}{k!}t^{-(a_1+\dots+a_k)}[\dots[V_{a_1},D_{a_20}],\dots,D_{a_k0}]$$
$$-\sum_{k\geqslant 1}\frac{1}{k!}\,t^{-(a_1+\dots+a_k)}[\dots[\sigma c_1,D_{a_10}],\dots,D_{a_k0}],$$

where in all last three sums the indices $a_1,\dots,a_k$ run over the set $\mathbb{Z}^0(p)$. The lifts $\tau_{<p}$ and the solutions $\{c_1\in\bar{\mathcal{L}}_{\mathcal{K}},\{V_{a0}\in\bar{\mathcal{L}}_k\mid a\in\mathbb{Z}^0(p)\}\}$ of (0.3) can be recovered uniquely one from another. In particular, c_1 is a strict invariant of a lift $\tau_{<p}$.

State the main results of this paper.

Suppose $c_1=\sum_{m\in\mathbb{Z}}c_1(m)t^m$, where all $c_1(m)\in\bar{\mathcal{L}}_k$.

Consider $\omega^p=\sum_{j\geqslant 0}A_jt^{e^*+pj}$, $A_j\in k$, from e) and $\widetilde{N}(e^*)$ from c).

Let $\bar{\mathcal{L}}^{(e^*)}$ be the image of $\mathcal{L}^{(e^*)}$ in $\bar{\mathcal{L}}$.

Theorem 0.1. *$\tau_{<p}$ is "good" iff*

$$c_1(0)\equiv\sum_{j\geqslant 0}\sum_{i=0}^{\widetilde{N}(e^*)-1}\sigma^i(A_j\mathcal{F}^0_{e^*+pj,-i})\bmod\bar{\mathcal{L}}_k^{(e^*)}\,.$$

Theorem 0.2. a) *If $v>e^*$ then $\Gamma^{(v)}_{<p}=G(L^{(v)})$, where $L^{(v)}$ is the image of $\mathcal{L}^{(v^*)}$ in $\bar{\mathcal{L}}\subset L$ and $v^*=e^*+p(v-e^*)$;*

b) *if $v\leqslant e^*$ and $\tau_{<p}$ is "good" then $\Gamma^{(v)}_{<p}=G(L^{(v)})$, where $L^{(v)}$ is generated by the image of $\mathcal{L}^{(v)}$ in $\bar{\mathcal{L}}$ and $\tau_{<p}$.*

Theorem 0.3. *If $2\leqslant s<p$ then $v[s]=e_K(1+s/(p-1))-1/p$.*

Remark. $v[1]=e^*(=e_K(1+1/(p-1))$ is a well-known fact at the level of abelian field extensions.

Consider the set of all $(a_1,n_1,\dots,a_s,n_s)$, where all $a_i\in\mathbb{Z}^0(p)$, $n_i\in\mathbb{Z}$ are such that $n_1\geqslant n_2\geqslant\dots\geqslant n_s=0$ and $\sum_{1\leqslant i\leqslant s}[a_i/e^*]\leqslant p-1-s$.

Let $\delta^+(e^*)$ be the minimum of positive values of

$$(e^*+pj)-p^{-n_1}(a_1p^{n_1}+\dots+a_sp^{n_s})\,,$$

where $(a_1,n_1,\dots,a_s,n_s)$ runs over the set of above defined vectors and j runs over the set of all non-negative integers. Set

$$N^+(e^*)=\min\{n\in\mathbb{N}\mid p^n\delta^+(e^*)\geqslant e^*(p-1)\}\,.$$

Fix $N^0\geqslant N^+(e^*)-1$ and set $\Omega^0=\sum_{j\geqslant 0}A_j\mathcal{F}^0_{e^*+pj,-N^0}$.

Introduce the operators F_0 and G_0 on $\bar{\mathcal{L}}_k$ such that for any $l\in\bar{\mathcal{L}}_k$,

$$F_0(l)=\sum_{1\leqslant k<p}\frac{\alpha_0^{k-1}}{k!}[\dots[l,\underbrace{D_0],\dots,D_0}_{k-1\text{ times}}],\ G_0(l)=\sum_{0\leqslant k<p}\frac{\alpha_0^k}{k!}[\dots[l,\underbrace{D_0],\dots,D_0}_{k\text{ times}}]\,.$$

Consider the relation

$$(0.4) \qquad (G_0\sigma - \mathrm{id})c^0 + F_0(V_0) = -G_0\sigma^{N^0+1}\Omega^0 .$$

Theorem 0.4. a) *There is a bijection between the lifts $\tau_{<p}$ and solutions (c^0, V_0) of* (0.3)*, with $c^0 \in \bar{\mathcal{L}}_k$ and $V_0 \in \bar{\mathcal{L}}$.*

b) *If $\tau_{<p}$ corresponds to (c^0, V_0) then the Demushkin relation appears in the form $(\mathrm{ad}\,\tau_{<p})D_0 = V_0$;*

c) *If $N^0 \geqslant \widetilde{N}(e^*)$ then $\tau_{<p}$ is "good" if and only if $c^0 \in \bar{\mathcal{L}}_k^{(e^*)}$.*

Corollary 0.5. a) *For any lift $\tau_{<p}$,*

$$(\mathrm{ad}\,\tau_{<p})D_0 + \sum_{0\leqslant n<N_0} \sigma^n(\Omega^0) \in [\bar{\mathcal{L}}, D_0];$$

b) *if $k = \mathbb{F}_p$ then there is a "good" lift $\tau_{<p}$, such that the Demushkin relation appears in the form $(\mathrm{ad}\tau_{<p})D_0 + F_0^{-1}(\Omega^0) = 0$.*

0.2. **Concluding remarks.** Our description of $\Gamma_{<p}$ together with its ramification filtration may serve as a guide to what a nilpotent local class field theory should be about. Our approach gives the objects of this theory on the level of groups of nilpotent class $< p$ together with induced ramification filtration. Regretfully, our description is not functorial: it depends on a choice of uniformizer in K.

It would be very interesting to compare our results with the construction of Γ in [9], cf. also [8]. This construction uses iterations of the Lubin-Tate theories via the field-of-norms functor and is done inside the group of formal power series with the operation given by their composition. However, it is not clear how to extract from that construction even well-known properties of the Galois group of a maximal p-extension of K.

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

1. Arithmetical lifts

1.1. **Review of ramification theory.** The following brief sketch of ramification theory of continuous automorphisms of complete discrete valuation fields with finite residue field of characteristic p (we need only this case) is based on the papers [7, 11, 12].

Let $\mathcal{E}$ be a basic complete discrete valuation field with finite residue field $k_{\mathcal{E}}$. Let $R_0(\mathcal{E})$ be the completion of a separable closure $\mathcal{E}_{sep}$ of $\mathcal{E}$. Note that in the characteristic 0 case, $R_0(\mathcal{E}) = \mathbb{C}_p$, and in the characteristic p case, $R_0(\mathcal{E}) = \mathrm{Frac}R := R_0$ is the field of fractions of Fontaine's ring $R = \varprojlim O_{\mathbb{C}_p}/p$ (the projective limit is taken with respect to the p-power maps).

Denote by $v_{\mathcal{E}}$ the extension of the normalized valuation on $\mathcal{E}$ to R_0. Let $\mathcal{I}$ be the group of all continuous automorphisms of R_0 which are compatible with $v_{\mathcal{E}}$ and induce the identity on the residue field of R_0.

Agree that all fields below E, F, L etc, are finite extensions of $\mathcal{E}$ in $\mathcal{E}_{sep}$ and use the appropriate notation v_E, k_E, etc. Let m_E be the maximal ideal of the valuation ring of E. Note that the inertia subgroup Γ_E^0 of $\Gamma_E = \mathrm{Gal}(\mathcal{E}_{sep}/E)$ is a subgroup in $\mathcal{I}$.

Let $\mathcal{I}_E = \{\iota|_E \mid \iota \in \mathcal{I}\}$.

For $g \in \mathcal{I}_E$, let $v(g) = \min\,\{v_E(g(a) - a) \mid a \in \mathrm{m}_E\} - 1$.

For $x \geqslant 0$, set $\mathcal{I}_{E,x} = \{g \in \mathcal{I}_E \mid v(g) \geqslant x\}$.

For a field extension F/E, let $\mathcal{I}_{F/E} = \{\iota \in \mathcal{I}_F \mid \iota|_E = \mathrm{id}_E\}$. For $x \geqslant 0$, let

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

If $\iota_1, \iota_2 \in \mathcal{I}_{F/E}$ and $x \geqslant 0$ then ι_1 and ι_2 are *x-equivalent* iff for any $a \in \mathrm{m}_F$, $v_F(\iota_1(a) - \iota_2(a)) \geqslant 1 + x$. 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 F/E can be defined for all $x \geqslant 0$, 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 $x \geqslant 0$, $\varphi_{L/E}(x) = \varphi_{F/E}(\varphi_{L/F}(x))$;
- the last edge point of the graph of $\varphi_{F/E}$ is $(x(F/E), v(F/E))$, where

$$x(F/E) = \inf\,\left\{x \geqslant 0 \mid (\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x}) = |\mathcal{I}_{F/E}|\right\}$$

is the largest lower and $v(F/E) = \varphi_{F/E}(x(F/E))$ is the largest upper ramification numbers for the extension F/E.

The following proposition is just a direct adjustment of the appropriate fact from the classical ramification theory for finite Galois extensions.

Proposition 1.1. *Suppose $g \in \mathcal{I}_E$ and $v(g) = y$. Then*

$$\max\{v(f) \mid f \in \mathcal{I}_F,\ f|_E = g\} = \varphi_{F/E}^{-1}(y)\,.$$

Proof. We can assume that F/E is totally ramified of degree d.

Suppose θ is a uniformizing element in F and $P(T) \in E[T]$ is its minimal monic polynomial over E. Then $P(T) = T^d + a_1 T^{d-1} + \cdots + a_d$ is an Eisenstein polynomial and $v(g) = v_E(g(a_d) - a_d) - 1 = y$.

Note that for all $1 \leqslant i < d$, $v_E(g(a_i)\theta^{d-i} - a_i\theta^{d-i}) > v_E(g(a_d) - a_d)$, Therefore, $v_E(g_* P(\theta)) = v_E(g_*(P)(\theta) - P(\theta)) = 1 + y$.

Let $\theta_1, \dots, \theta_d$ be all roots of $g_* P(T)$ in $\hat{E}_{sep}$. Then all d different lifts f_i of g to F are uniquely determined by the condition $f_i(\theta) = \theta_i$, $i = 1, \dots, d$. Clearly, $v(f_i) = v_F(\theta - \theta_i) - 1$.

Assume that $x = v(f_1)$ is maximal, i.e. $1 + x \geqslant v_F(\theta - \theta_i)$ for all i. It remains to prove that $y = \varphi_{F/E}(x)$.

Let $A_i := v_F(\theta_i - \theta_1) - 1 \geqslant 0$. Note $A_1 = +\infty$. Then

$$v_F(g_*P(\theta)) = \sum_{1\leqslant i\leqslant d} v_F(\theta - \theta_i) = \sum_{1\leqslant i\leqslant d} \min\{1+x, 1+A_i\} = d + \varphi(x)$$

The function $\varphi(x) = \sum_{1\leqslant i\leqslant d} \min\{x, A_i\}$ is peace-wise linear, $\varphi(0) = 0$ and if x is different from all A_i then

$$\varphi'(x) = |\{A_i \mid A_i > x\}| = |\mathcal{I}_{F/E,x}| = (\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x})^{-1} d = d\varphi'_{F/E}(x)\,.$$

Therefore, $\varphi(x) = d\varphi_{F/E}(x)$ and, finally, $1 + y = v_E(g_*P(\theta)) = d^{-1}v_F(g_*P(\theta)) = d^{-1}(d + d\varphi_{F/E}(x)) = 1 + \varphi_{F/E}(x)$. □

Corollary 1.2. *The restriction $\mathcal{I}_F \longrightarrow \mathcal{I}_E$ given by the correspondence $f \mapsto g := f|_E$ defines for any $x_0 \geqslant 0$, the surjection $\mathcal{I}_{F,x_0} \longrightarrow \mathcal{I}_{E,y_0}$, where $y_0 = \varphi_{F/E}(x_0)$.*

Proof. Let $f \in \mathcal{I}_{F,x_0}$ and $v(g) = y$. By Proposition 1.1, $x_0 \leqslant v(f) \leqslant \varphi^{-1}_{F/E}(y)$. This implies that $y_0 \leqslant y$, i.e. $g \in \mathcal{I}_{E,y_0}$.

On the other hand, if $g \in \mathcal{I}_{E,y_0}$ then $v(g) = y \geqslant y_0$ and by Proposition 1.1 there is $f \in \mathcal{I}_{F,\varphi^{-1}_{F/E}(y)} \subset \mathcal{I}_{F,x_0}$ such that $g = f|_E$. □

Definition. The ramification filtration $\{\mathcal{I}^{(y)}_{/E}\}_{y\geqslant 0}$ on $\mathcal{I}$ with upper numbering over E is a decreasing sequence of the subsets $\mathcal{I}^{(y)}_{/E} \subset \mathcal{I}$ for all $y \geqslant 0$, such that

$$\mathcal{I}^{(y)}_{/E} = \{\iota \in \mathcal{I} \mid \forall\, F/E,\ \iota|_F \in \mathcal{I}_{F,\varphi^{-1}_{F/E}(y)}\}\,.$$

Note that for any $y \geqslant 0$, $\mathcal{I}^{(y)}_{/E} = \mathcal{I}^{(y_F)}_{/F}$, where $\varphi_{F/E}(y_F) = y$. Also, $\Gamma^{(y)}_E := \Gamma_E \cap \mathcal{I}^{(y)}_{/E}$ is the usual higher ramification subgroup $\Gamma^{(y)}_E$ of Γ_E with the upper number y from [10]. The largest ramification number $v(F/E)$ is characterized by the following property:

- *the ramification subgroup $\Gamma^{(y)}_E$ acts trivially on F iff $y > v(F/E)$.*

1.2. **Definition of arithmetical lifts.**

Definition. For a field extension F/E we say that $f \in \mathcal{I}_F$ is arithmetical over E (or f is an arithmetical lift of $g = f|_E$) if $v(g) = \varphi_{F/E}(v(f))$. Equivalently, f is arithmetical over E if there is $\iota \in \mathcal{I}^{(v(g))}_{/E}$ such that $\iota|_F = f$.

Note that Corollary 1.2 implies that f is arithmetical over E iff $v(f) = \max\{v(f') \mid f' \in \mathcal{I}_F\,, f'|_E = g\}$. In particular, arithmetical lifts always exist.

Proposition 1.1 and Corollary 1.2 imply the following property.

Proposition 1.3. *Suppose $E \subset L \subset F$ are finite field extensions and $f \in \mathcal{I}_F$. Then:*

a) *f is arithmetical over E iff f is arithmetical over L and $f|_L$ is arithmetical over E;*

b) *suppose F/E is Galois, $f, f' \in \mathcal{I}_F$ are such that $f|_E = f'|_E = g$ and f is arithmetical over E; then f' is arithmetical over E iff there is $\tau \in \Gamma_E^{(v(g))}$ such that $f' = f \cdot \tau|_F$.*

Proof. The part a) follows from the composition property of the Herbrand function. As for the part b), note that $f = \iota|_F$, where $\iota \in \mathcal{I}_{/E}^{(v(g))}$ and there is $\tau \in \Gamma_E$ such that for $\iota' := \iota\tau$, we have $f' = \iota'|_F$. We must verify that

- $\iota' \in \mathcal{I}_{/E}^{(v(g))}$ iff $\tau \in \mathcal{I}_{/E}^{(v(g))} \cap \Gamma_E = \Gamma_E^{(v(g))}$.

Suppose $\iota' \in \mathcal{I}_{/E}^{(v(g))}$. Then for any finite field extension E'/E, and any $a \in \mathrm{m}_{E'}$, we have that

$$\varepsilon' := \varphi_{E'/E}^{-1}(v(g)) + 1 \leqslant v_{E'}(\iota'(a) - a) = v_{E'}(\iota(\tau a - a) + (\iota(a) - a))\,.$$

But $v_{E'}(\iota(a) - a) \geqslant \varepsilon'$ (use that $\iota \in \mathcal{I}_{/E}^{(v(g))}$) implies $v_{E'}(\tau a - a) \geqslant \varepsilon'$ and, therefore, $\tau \in \Gamma_E^{(v(g))}$.

Inversely, if $\tau \in \Gamma_E^{(v(g))}$ and $a \in \mathrm{m}_{E'}$ then $v_{E'}(\tau a - a) \geqslant \varepsilon'$ and $v_{E'}(\iota'(a) - a) = v_{E'}(\iota(\tau a - a) + \iota(a) - a) \geqslant \varepsilon'$, i.e. $\iota' \in \mathcal{I}_{/E}^{(v(g))}$. □

As a direct application of the above proposition note the following.

Suppose $g \in \mathcal{I}_E$, $v_g = v(g)$ and $\mathcal{E}^{(v_g)} \subset \mathcal{E}_{sep}$ is the subfield fixed by $\Gamma_E^{(v_g)}$. We will call $f \in \mathcal{I}$ arithmetical over E if for any finite extension F/E the restriction $f|_F$ is arithmetical over E.

Corollary 1.4. a) *$\iota \in \mathcal{I}$ is arithmetical lift of $g = \iota|_E$ if and only if $\iota^{(v_g)} := \iota|_{\mathcal{E}^{(v_g)}}$ is arithmetical over E;*

b) *$\iota^{(v_g)}$ is a unique arithmetical lift of g to $\mathcal{E}^{(v_g)}$.*

Proof. Suppose F/E is Galois, $\mathrm{Gal}(F/E) = \Gamma$, $F^{(v_g)} = F^{\Gamma^{(v_g)}}$, $f \in \mathcal{I}_F$, $f|_E = g$ and $f|_{F^{(v_g)}} = f^{(v_g)}$.

If f is arithmetical over E then by Proposition 1.3a) $f^{(v_g)}$ is also arithmetical over E.

Inversely, suppose $f^{(v_g)}$ is arithmetical over E and $f' \in \mathcal{I}_F$ is arithmetical lift of $f^{(v_g)}$ to F. Then there is $\tau \in \mathrm{Gal}(F/F^{(v_g)}) = \Gamma^{(v_g)}$ such that $f = f'\tau$ and by Proposition 1.3b) f is arithmetical over E. This proves a) of our proposition.

Suppose $h, h' \in \mathcal{I}_{F^{(v_g)}}$ are lifts of g. Then there is $\tau \in \Gamma_{F^{(v_g)}} := \mathrm{Gal}(F^{(v_g)}/E)$ such that $h' = h\tau$. If h, h' are arithmetical over E then by Proposition 1.3b), $\tau \in \Gamma_{F^{(v_g)}}^{(v_g)} = \{e\}$ and $h = h'$. □

2. Characterization of arithmetical lifts

2.1. **Differentials of lifts.** In this Section we review the results from Sections 2 and 3 of [6]. Recall, we have the identification $\eta_0 : \mathcal{G}_{<p} = \mathrm{Gal}(\mathcal{K}_{<p}/\mathcal{K}) \simeq G(\mathcal{L})$, given via $\eta_0(\tau) = (-f)\circ\tau(f)$, where $e = \sum_{a\in\mathbb{Z}^0(p)} t^{-a}D_{a0} \in \mathcal{L}_{\mathcal{K}}$ and $f \in \mathcal{L}_{\mathcal{K}_{sep}}$ are such that $\sigma f = e\circ f$. There is a decreasing central filtration $\{\mathcal{L}(s)\}_{s\geqslant 1}$ in $\mathcal{L}$ such that $D_{an}\in\mathcal{L}(s)$ if $a\geqslant (s-1)c_0$, where $c_0\in p\mathbb{N}$. We have also $h\in \mathrm{Aut}\,\mathcal{K}$ such that $h|_k = \mathrm{id}$ and $h(t) = t\widetilde{\exp}(\omega_h(t)^p)$, where $\omega_h(t)\in t^{c_0/p}k[[t]]^*$.

2.1.1. Let $h_{<p}$ be a lift of h to $\mathcal{K}_{<p}$. Then there are 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 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

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

If $c = \sum_{i\in\mathbb{Z}} t^i c(i)$, where all $c(i)\in\mathcal{L}_k$ then $c(0)$ is a strict invariant of the lift $h_{<p}$. Consider

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

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

where m and $\mathrm{m}_{<p}$ are the maximal ideals of the valuation rings of $\mathcal{K}$ and, resp., $\mathcal{K}_{<p}$. Then $\mathcal{M}\subset\mathcal{M}_{<p}$ is embedding of Lie $\mathbb{F}_p$-algebras, $e\in\mathcal{M}$ and $f\in\mathcal{M}_{<p}$.

Define the decreasing filtration by ideals $\mathcal{M}[i]$, $i\geqslant 0$, of $\mathcal{M}$ by setting $\mathcal{M}[0] := \mathcal{M}$ and for $i\geqslant 1$, $\mathcal{M}[i] := \mathcal{L}(i)_k + t^{c_0 i}\mathcal{M}$. Then $\mathcal{M}_{<p}[i] := \mathcal{M}[i] + t^{c_0 i}\mathcal{M}_{<p}$, $i\geqslant 0$, is a decreasing filtration of ideals in $\mathcal{M}_{<p}$. Note that for all i, $\mathcal{M}[i] = \mathcal{M}\cap\mathcal{M}_{<p}[i]$.

Consider the embedding of Lie $\mathbb{F}_p$-algebras

$$\bar{\mathcal{M}} := \mathcal{M}/\mathcal{M}(p-1)\subset\bar{\mathcal{M}}_{<p} := \mathcal{M}_{<p}/\mathcal{M}_{<p}(p-1)\,,$$

where $\mathcal{M}(p-1) = t^{c_0(p-1)}\mathcal{M}$ and $\mathcal{M}_{<p}(p-1) = t^{c_0(p-1)}\mathcal{M}_{<p}$. The images of the above filtrations $\mathcal{M}[i]$ and $\mathcal{M}_{<p}[i]$ in the quotients $\bar{\mathcal{M}}$ and $\bar{\mathcal{M}}_{<p}$ will be denoted by $\bar{\mathcal{M}}[i]$ and $\bar{\mathcal{M}}_{<p}[i]$. Note that $\bar{M}[p] = \mathcal{M}_{<p}[p] = 0$. Denote by $\bar{f}$ and $\bar{e}$ the images of f and e in $\bar{\mathcal{M}}_{<p}$ and $\bar{\mathcal{M}}$.

2.1.2. Let $\mathcal{K}(p) := \mathcal{K}_{<p}^{G(\mathcal{L}(p))}$ and $h(p) := h_{<p}|_{\mathcal{K}(p)}$. Then η_0 induces the identification $\bar{\eta}_0 : \mathrm{Gal}(\mathcal{K}(p)/\mathcal{K})\simeq G(\bar{\mathcal{L}})$. Note that $\bar{\eta}_0(\tau) = (-\bar{f})\circ\tau(\bar{f})$ (use that $\bar{\mathcal{L}} = \bar{\mathcal{M}}_{<p}|_{\sigma=\mathrm{id}}$).

Let $\widetilde{\mathcal{G}}_h$ be the subgroup generated by all lifts $h_{<p}$ in $\mathrm{Aut}\mathcal{K}_{<p}$. Then $C_p(\widetilde{\mathcal{G}}_h) = G(\mathcal{L}(p))$, $\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h)\subset\mathrm{Aut}\mathcal{K}(p)$, and there is an exact sequence of p-groups

$$0\longrightarrow G(\bar{\mathcal{L}})\longrightarrow\mathcal{G}_h\longrightarrow\langle h\rangle^{\mathbb{Z}/p}\longrightarrow 1\,,$$

where $\mathcal{G}_h = \widetilde{\mathcal{G}}_h / C_p(\widetilde{\mathcal{G}}_h)\widetilde{\mathcal{G}}_h^p$ is the maximal quotient of $\widetilde{\mathcal{G}}_h$ of nilpotent class $< p$ and period p. This sequence appears also at the level of Lie $\mathbb{F}_p$-algebras in the form

$$0 \longrightarrow \bar{\mathcal{L}} \longrightarrow L_h \longrightarrow \mathbb{F}_p h \longrightarrow 0\,,$$

where $G(L_h) = \mathcal{G}_h$.

Proceeding in $\bar{\mathcal{M}}$ we specify the image of the lift $h(p)$ in $\mathcal{G}_h$ by setting $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p))\bar{f} = \bar{c} \circ (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}$ where $\bar{c} = c \bmod \mathcal{M}(p-1) \in \bar{\mathcal{M}}$ and $\bar{A} = A \bmod \mathcal{L}(p) = \mathrm{Ad}\, h(p) = \widetilde{\exp}(\mathrm{ad}\, h(p))$. Then for $n \in \mathbb{N}$, $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^n)\bar{f} = \bar{c}(n) \circ \bar{f}(n)$, with $\bar{f}(n)$ and $\bar{c}(n)$ such that:

a) $\bar{f}(n) = (\bar{A}^n \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f} = \bar{f} + \sum_{1 \leqslant i < p} \bar{f}^{(i)} n^i$, where for $1 \leqslant i < p$,

$$\bar{f}^{(i)} = (\mathrm{ad}^i h(p) \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}/i! \in (\bar{A} \otimes \mathrm{id}_{\mathcal{K}(p)} - \mathrm{id}_{\bar{\mathcal{M}}_{<p}})^i \bar{\mathcal{M}}_{<p} \subset \bar{\mathcal{M}}_{<p}[i]\,;$$

b) $\bar{c}(n) = \sum_{1 \leqslant i < p} c_i n^i \bmod \mathcal{M}(p-1)$, where all $c_i \in \mathcal{M}[i]$.

As a result, $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^n)\bar{f} = \bar{f} + \sum_{i \geqslant 1} \bar{f}_i n^i$, where all $\bar{f}_i \in \bar{\mathcal{M}}_{<p}[i]$.

2.1.3. Let $\bar{\mathcal{M}}^f$ be 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 $n \in \mathbb{N}$. Then $\bar{\mathcal{M}}^f$ does not depend on a choice of $h(p)$ and appears as the minimal subalgebra in $\bar{\mathcal{M}}_{<p}$ containing $\bar{\mathcal{M}}$ and all $\bar{f}^{(i)}$ (we set $\bar{f}^{(i)} = 0$ if $i \geqslant p$). Then $\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)$ acts on $\bar{\mathcal{M}}^f$, the resulting action of $\mathcal{G}_h$ on $\bar{\mathcal{M}}^f$ is strict, the filtration $\bar{\mathcal{M}}_{<p}[i]$ induces a $\mathcal{G}_h$-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 $\bar{\mathcal{M}}^f[i]$.

This gives the 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 the formal additive group $\mathbb{G}_{a,\mathbb{F}_p}$ on $\bar{\mathcal{M}}^f$ given via the relation

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f} = \bar{f} \otimes 1 + \sum_{i \geqslant 1} \bar{f}_i \otimes U^i$$

and this action can be uniquely recovered from its linear component (i.e. the differential) $d(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U) : \bar{\mathcal{M}}^f \longrightarrow \bar{\mathcal{M}}^f \otimes U$.

Note that $h^U(t) \equiv t\widetilde{\exp}(U\omega_h^p) \bmod t^{pc_0+1}$ and

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

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

$$\sigma\bar{c}_1 - \bar{c}_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_{a0} \equiv \tag{2.2}$$

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

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

$$-\sum_{k\geqslant 1}\frac{1}{k!}t^{-(a_1+\dots+a_k)}[\dots[\sigma\bar{c}_1, D_{a_10}],\dots,D_{a_k0}]$$

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

Any solution $\{\bar{c}_1, \{V_{a0}\mid a\in\mathbb{Z}^0(p)\}\}$ of congruence (2.2) modulo $\mathcal{M}(p-1)$ can be uniquely lifted to a solution $\{c_1,\{V_{a0}\mid a\in\mathbb{Z}^0(p)\}\}$ of (2.2) modulo $\mathcal{L}(p)_{\mathcal{K}}\subset\mathcal{M}(p-1)$. As a result, cf. [6], Subsection 3.5, the appropriate $c_1\in\bar{\mathcal{L}}_{\mathcal{K}}$ is a strict invariant of the lift $h(p)$. Even more, if $c_1=\sum_{i\in\mathbb{Z}}t^ic_1(i)$ where all $c_1(i)\in\bar{\mathcal{L}}_k$ then $c_1(0)$ is a strict invariant of $h(p)$.

2.2. **Statement of Criterion.** In this subsection we study arithmetical lifts $h_{<p}$ of h and prove that $h_{<p}$ is arithmetical iff $h(p)=h_{<p}|_{\mathcal{K}(p)}$ is arithmetical. This allows us to characterize arithmetical lifts in terms related to the differentials $d(\mathrm{id}_{\bar{\mathcal{L}}}\otimes h(p)^U)$.

Suppose $h_{<p}$ is arithmetical over $\mathcal{K}$.

By Corollary 1.4b) such lift $h_{<p}$ is unique modulo the ramification subgroup $\mathcal{G}^{(c_0)}_{<p}=G(\mathcal{L}^{(c_0)})$ (note that $v(h)=c_0$). Therefore, we can characterize arithmetical lifts $h_{<p}$ by studying the action of $h_{<p}$ on $f \bmod \mathcal{L}^{(c_0)}_{\mathcal{K}_{<p}}\in(\mathcal{L}/\mathcal{L}^{(c_0)})_{\mathcal{K}^{(c_0)}}$, where $\mathcal{K}^{(c_0)}:=\mathcal{K}^{G(\mathcal{L}^{(c_0)})}_{<p}$, cf. Section 1.3 of [6].

The following proposition provides us with the opportunity to characterize arithmetical lifts $h_{<p}$ by working with $\bar{f}=f \bmod \mathcal{M}_{<p}(p-1)$. (Recall that $\bar{f}$ allows us to control efficiently the lifts $h(p)=h_{<p}|_{\mathcal{K}(p)}$, cf. the beginning of Section 2.1.2.)

Proposition 2.1. $\mathcal{L}(p)\subset\mathcal{L}^{(c_0)}$.

Proof. Proposition follows easily from Lemma 2.3 below. □

Corollary 2.2. *$h_{<p}$ is arithmetical iff $h(p)$ is arithmetical (over $\mathcal{K}$).*

Proof. Indeed, use that both automorphisms are arithmetical over $\mathcal{K}$ iff $h_{<p}|_{\mathcal{K}^{(c_0)}}=h(p)|_{\mathcal{K}^{(c_0)}}:=h^{(c_0)}$ is arithmetical over $\mathcal{K}$. □

Lemma 2.3. *If $a\geqslant(s-1)c_0$ then $D_{an}\in\mathcal{L}^{(c_0)}_k+C_s(\mathcal{L}_k)$.*

Proof of lemma. This lemma was proved in [1] but the proof is very short and we shall reproduce it. Recall that $\mathrm{wt}(D_{an})\geqslant s$ means that $(s-1)c_0\leqslant a$. Use induction on s.

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

Assume $s\geqslant 2$ and the lemma is proved for all $s'<s$. Consider

$$\mathcal{F}^0_{a,-N}=aD_{a0}+(\text{ commutators of order}\geqslant 2)\in\mathcal{L}^{(c_0)}_k,$$

cf.[6], Subsection 1.4. This element is a linear combination of the commutators $a_1[\dots[D_{a_1n_1},D_{a_2n_2}],\dots,D_{a_tn_t}]$, where

a) $0=n_1\geqslant\dots\geqslant n_t\geqslant -N$;

b) $a=a_1p^{n_1}+\dots+a_tp^{n_t}$.

If for $1 \leqslant i \leqslant t$, $D_{a_i n_i} \in \mathcal{L}(s_i) \setminus \mathcal{L}(s_i+1)$ then

$$a \leqslant a_1 + \cdots + a_t < (s_1 + \cdots + s_t)c_0$$

and this implies $s \leqslant s_1 + \cdots + s_t$.

Suppose $t \geqslant 2$. Then $\mathrm{wt}(D_{a_i n_i}) \geqslant \min\{s_i, s-1\}$ and by the inductive assumption our commutator belongs to $\mathcal{L}_k^{(c_0)} + C_{s'}(\mathcal{L}_k)$, where $s' = \sum_{1\leqslant i\leqslant t} \min\{s_i, s-1\} \geqslant \min\{s_1 + \cdots + s_t, s\} = s$. □

As a result, the property for $h_{<p}$ to be arithmetical over $\mathcal{K}$ can be stated in terms of the differential $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes h(p)^U)\bar{f} = \bar{f}_1 \otimes U$ or, equivalently in terms of $(\mathrm{ad}\, h(p) \otimes \mathrm{id}_{\mathcal{K}(p)})\bar{f}$ and the linear part $\bar{c}_1 \in \bar{\mathcal{M}}[1]$ of $\bar{c}(U)$, cf. Subsection 2.1.

Note that if $h_{<p}$ is arithmetical then for any $g \in \mathcal{G}_{<p}$, $h_{<p}^{-1}\, g\, h_{<p} \equiv g \bmod \mathcal{G}^{(c_0)}$. (Indeed, $g^{-1}h_{<p}g$ is another lift of h which is also arithmetical and, therefore, it coincides with $h_{<p}$ modulo $\mathcal{G}_{<p}^{(c_0)}$.) Therefore, $\mathrm{Ad}h_{<p} \equiv \mathrm{id}_{\mathcal{L}} \bmod \mathcal{L}^{(c_0)}$. In particular,

$$(\mathrm{Ad}h_{<p} \otimes \mathrm{id}_{\mathcal{K}_{<p}})f \equiv f \bmod \mathcal{L}_{\mathcal{K}_{<p}}^{(c_0)}$$

is a necessary condition for $h_{<p}$ to be arithmetical. It is natural to expect that a sufficient condition for $h_{<p}$ to be arithmetical over $\mathcal{K}$ requires additional condition which can be stated in terms of $\bar{c}_1 \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)}$. Even more, we are going to establish this condition in terms related only to $c_1(0) \in \mathcal{L}_k \bmod \mathcal{L}_k^{(c_0)}$, where we set $\bar{c}_1 = \sum_{m\in\mathbb{Z}} c_1(m)t^m \bmod \mathcal{M}(p-1)$ with all $c_1(m) \in \mathcal{L}_k$.

Theorem 2.4. *The following properties are equivalent:*

a) $h_{<p}$ *is arithmetical over* $\mathcal{K}$*;*

b) $(\mathrm{Ad}h_{<p} - \mathrm{id}_{\mathcal{L}})\mathcal{L} \subset \mathcal{L}^{(c_0)}$ *and for a sufficiently large* N*,*

$$\bar{c}_1 \equiv \sum_{\gamma,j} \sum_{0\leqslant i<N} \sigma^i(A_j(h)\mathcal{F}^0_{\gamma,-i}t^{-\gamma+c_0+pj}) \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{M}(p-1)\,;$$

c) *for a sufficiently large* N*,*

$$c_1(0) \equiv \sum_{j\geqslant 0} \sum_{0\leqslant i<N} \sigma^i(A_j(h)\mathcal{F}^0_{c_0+pj,-i}) \bmod \mathcal{L}_k^{(c_0)}\,.$$

The proof will be given in Subsections 2.4-2.7 below.

Remark. Note that if $\gamma \geqslant c_0$ and $i \geqslant \widetilde{N}(c_0)$, cf. [6], Theorem 1.2, then $\mathcal{F}^0_{\gamma,-i} \in \mathcal{L}_k^{(c_0)}$. There is also $\delta > 0$, cf. Section 2.3 below, such that if $\mathcal{F}^0_{\gamma,-i} \notin \mathcal{L}_k^{(c_0)}$ and $\gamma < c_0$ then $\gamma < c_0 - \delta$. (In other words, any $\gamma \in [c_0 - \delta, c_0)$ can't be presented in the form $a_1 + a_2p^{n_2} + \cdots + a_sp^{n_s}$, where $1 \leqslant s < p$, all $n_j \leqslant 0$ and all $a_j \in \mathbb{Z}^0(p) \cap [0, (p-1)c_0)$.) Therefore, in b) we can take $N \geqslant \max\{\widetilde{N}(c_0), \log_p((p-1)c_0/\delta)\}$ and in c) $N \geqslant \widetilde{N}(c_0)$ (under these conditions the appropriate RHS's do not depend on N).

2.3. **Auxiliary result.** We review here a technical result from [3], Section 3. (Note that all results in [3] were obtained in the contravariant setting, cf. discussion in [6], Subsection 1.1) This paper deals with explicit calculations with ramification ideals in Lie algebras over $\mathbb{Z}/p^{M+1}$. It is much easier to follow these calculations when assuming that $M=0$ (we need only this case). First, introduce the relevant objects and assumptions.

Introduction of 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 $A=[0,(p-1)v_0)\cap\mathbb{Z}^0(p)$, where $v_0\geqslant 0$ (later we shall specify $v_0=c_0$). (In [3] we used pv_0 in the definition of A instead of $(p-1)v_0$ but everything works with $(p-1)v_0$.) Let $\mathcal{L}(A)$ be a free Lie algebra over $k\simeq\mathbb{F}_{p^{N_0}}$ with the set of generators

$$\{\mathcal{D}_{an}\mid a\in A^+=A\cap\mathbb{Z}^+(p), n\in\mathbb{Z}/N_0\}\cup\{\mathcal{D}_0\}\,.$$

As a matter of fact, we agreed in [3] that $n\in\mathbb{Z}$ and $\mathcal{D}_{an_1}=\mathcal{D}_{an_2}$ iff $n_1\equiv n_2 \bmod N_0$. For $n\in\mathbb{Z}$, set $\mathcal{D}_{0n}=(\sigma^n\alpha_0)\mathcal{D}_0$ and note that again $\mathcal{D}_{0n}$ depends only on $n \bmod N_0$. Consider the σ-linear morphism $\mathcal{L}(A)\longrightarrow\mathcal{L}(A)$ such that for all a and n, $\mathcal{D}_{an}\mapsto\mathcal{D}_{a,n+1}$ and denote this morphism also by σ. Then $\mathcal{L}^0:=\mathcal{L}(A)|_{\sigma=\mathrm{id}}$ is a free Lie algebra over $\mathbb{F}_p$ and $\mathcal{L}^0_k=\mathcal{L}(A)$.

Consider the contravariant analogue of the elements $\mathcal{F}^0_{\gamma,-N}$ from [6], Subsection 1.4, (use the same conditions for all involved indices)

$$\mathcal{F}_{\gamma,-N}=\sum_{1\leqslant s<p}(-1)^{s-1}\sum_{\substack{a_1,\dots,a_s\\ n_1,\dots,n_s}}a_1\eta(n_1,\dots,n_s)[\dots[\mathcal{D}_{a_1n_1},\mathcal{D}_{a_2n_2}],\dots,\mathcal{D}_{a_sn_s}]\,.$$

Recall that $a_1,\dots,a_s$ run over A and $n_1,\dots,n_s$ run over $\mathbb{Z}$ such that $\gamma(\bar a,\bar n)=a_1p^{n_1}+\dots+a_sp^{n_s}=\gamma$.

Denote by $\mathcal{L}^0_N(v_0)$ the minimal ideal in $\mathcal{L}^0$ such that its extension of scalars $\mathcal{L}^0_N(v_0)_k$ contains all $\mathcal{F}_{\gamma,-N}$ with $\gamma\geqslant v_0$. Let $\widetilde{N}(v_0,A)$ be such that the ideals $\mathcal{L}^0_N(v_0)$ coincide for all $N\geqslant\widetilde{N}(v_0,A)$ and denote this ideal by $\mathcal{L}^0(v_0)$.

Let $\Gamma=\Gamma(A,v_0)$ be the set of all $\gamma=a_1p^{n_1}+\dots+a_sp^{n_s}$, where all $a_i\in A$, $0=n_1\geqslant n_2\geqslant\dots\geqslant n_s$, $1\leqslant s<p$.

Choice of parameters δ, r^*, N^*:

a) let $\delta=\delta(A,v_0)>0$ be sufficiently small such that $v_0-\delta>\max\{\gamma\mid\gamma\in\Gamma,\gamma<v_0\}$, $p\delta<2v_0$ and $v_0-\delta\in\mathbb{Z}[1/p]$;

b) let $r^*\in\mathbb{Q}$ be such that $v_p(r^*)=0$ and $v_0-\delta<r^*<v_0$;

c) let $N^*\in\mathbb{N}$ be such that $N^*\geqslant\widetilde{N}(v_0,A)+1$ and for $q=p^{N^*}$, we have $r^*(q-1)=b^*\in\mathbb{N}$ (note $v_p(b^*)=0$), $a^*=q(v_0-\delta)\in p\mathbb{N}$;

d) note that if q satisfies the conditions from c) then any its power q^A with $A\in\mathbb{N}$ also satisfies these conditions; therefore, we can enlarge (if necessary) q to obtain the following inequalities:

$$r^*-(v_0-\delta)>\frac{r^*+p(v_0-\delta)}{q}\,,\quad v_0-r^*>\frac{-r^*+\varphi_{(p)}(e_{(p)}v_0(p-1))}{q}$$

All above constructions and choices were made in Section 3.1 of [3], except the additional conditions $p\delta<2v_0$ and the second inequality in d). In this inequality $\varphi_{(p)}$ and $e_{(p)}$ are the Herbrand function and, resp., the ramification index of the extension $\mathcal{K}(p)/\mathcal{K}$. Recall that $\mathcal{K}(p)$ is a subfield of $\mathcal{K}_{<p}$, fixed by $G(\mathcal{L}(p))$ and $[\mathcal{K}(p):\mathcal{K}]<\infty$.

We need the 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 (r^*,r^*);

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

The field $\mathcal{K}'$ played very important role in our approach to the ramification filtration, cf. e.g. [1, 2, 3, 4]. (Note that $\mathcal{K}'/\mathcal{K}$ is not a p-extension if $N^*>1$.)

Adjust the notation from [3] to our situation by setting $\hat N=\widetilde N=N^*-1$ (in particular, $\widetilde N$ could be different from $\widetilde N(v_0,A)$ introduced earlier).

Let $\hat e^{(0)}_{\mathcal{L}}=\sum_{a\in A}t^{-a}\mathcal{D}_{a0}$ and $e'^{(q)}_{\mathcal{L}}=\sum_{a\in A}{t'}^{-aq}\mathcal{D}_{a0}$. (We follow maximally close the notation from [3].) Clearly, the elements $\hat e^{(0)}_{\mathcal{L}}$ and $e'_{\mathcal{L}}:=\sum_{a\in A}{t'}^{-a}\mathcal{D}_{a,-N^*}$ are analogs of our element $e\in\mathcal{L}_{\mathcal{K}}$ and $\sigma^{N^*}e'_{\mathcal{L}}=e'^{(q)}_{\mathcal{L}}$. Note that both these elements belong to $\mathcal{L}^0_{\mathcal{K}'}=\mathcal{L}(A)\otimes_k\mathcal{K}'$ (for $\hat e^{(0)}_{\mathcal{L}}$ use that $t=t'^qE(t'^{b^*})^{-1}$).

The technical result from [3] we are going to apply below deals with estimates in the envelopping algebra $\mathcal{A}$ of $\mathcal{L}^0$. We can describe this result as follows.

Let J be the augmentation ideal in $\mathcal{A}$. Adjusting the notation from [3] note that (since we work with the case $M=0$) $O_1=\mathcal{K}'$, $t_1=t'$, $O_0=k[[t']]$, $J_1=J_{\mathcal{K}'}$ and $J_O=J\otimes O_0$.

Use the map $\widetilde{\exp}$ from $\mathcal{L}^0_{\mathcal{K}'}$ to $J_{\mathcal{K}'}\operatorname{mod}J^p_{\mathcal{K}'}$, cf. [6], the beginning of Subsection 3.3. We obtain the elements $E_0=\widetilde{\exp}(\hat e^{(0)}_{\mathcal{L}})$, $E'_0=\sigma^{N^*}\widetilde{\exp}(e'_{\mathcal{L}})$ and (where we specified $m=1$) the element $\Phi_0^{(\widetilde N)}=\Phi_{01}^{(\widetilde N)}=\Phi_{11}\Phi_{21}$, cf. the first paragraph on p.890 in the proof of Lemma 2 in Subsection 3.10 of [3]. Explicit expressions for Φ_{11} and Φ_{21} from the second paragraph on p.890 must be written in the following way

$$\Phi_{11}=\widetilde{\exp}(e'^{(q)}_{\mathcal{L}})\,\widetilde{\exp}(\sigma e'^{(q)}_{\mathcal{L}})\,\dots\,\widetilde{\exp}(\sigma^{\widetilde N}e'^{(q)}_{\mathcal{L}})$$

$$\Phi_{21}=\widetilde{\exp}(-\sigma^{\widetilde N}\hat e^{(0)}_{\mathcal{L}})\,\dots\,\widetilde{\exp}(-\sigma\hat e^{(0)}_{\mathcal{L}})\,\widetilde{\exp}(-\hat e^{(0)}_{\mathcal{L}})\,.$$

(By misprint they appeared in [3] as the products of the same factors but taken in the opposite order.) Note that when adjusting the notation from [3] to our situation we have that $\mathcal{E}_{0-\hat{N}}(a,n)=\sigma^nE(a,t'^{b^*})$ and, therefore, $\mathcal{E}_{0-\hat{N}}(a,n)\sigma^n(t_1^{-qa}\mathcal{D}_{a0})$ coincides with $\sigma^n(t^{-a}\mathcal{D}_{a0})$.

Using properties $\alpha)-\gamma)$ from Subsection 3.3 of [6] we obtain that $\Phi_0^{(\tilde{N})}=\widetilde{\exp}(\phi_0^{(\tilde{N})})$, where $\phi_0^{(\tilde{N})}\in G(\mathcal{L}^0_{\mathcal{K}'})=G(\mathcal{L}(A)\otimes_k\mathcal{K}')$ is equal to

$$\phi_0^{(\tilde{N})}=e'^{(q)}_{\mathcal{L}}\circ(\sigma e'^{(q)}_{\mathcal{L}})\circ\dots\circ(\sigma^{\tilde{N}}e'^{(q)}_{\mathcal{L}})\circ(-\sigma^{\tilde{N}}\hat{e}^{(0)}_{\mathcal{L}})\circ\dots\circ(-\sigma\hat{e}^{(0)}_{\mathcal{L}})\circ(-\hat{e}^{(0)}_{\mathcal{L}})\,.$$

Then properties (a) and (b) of $\Phi_0^{(\tilde{N})}$ from Proposition 9 of Subsection 3.9 in [3] imply the following properties of the element $\phi_0^{(\tilde{N})}$, cf. the proposition from Subsection 3.10 of [3] (where $\mathcal{L}_O:=\mathcal{L}^0\otimes O_0$).

Proposition 2.5. *a)* $\phi_0^{(\tilde{N})},\sigma\phi_0^{(\tilde{N})}\in\mathcal{L}^0(v_0)_{\mathcal{K}'}+\sum_{1\leqslant j<p}t'^{-ja^*}C_j(\mathcal{L}_O)$;

b) $\phi_0^{(\tilde{N})}\circ\hat{e}^0_{\mathcal{L}}\equiv e'^{(q)}_{\mathcal{L}}\circ\sigma\phi_0^{(\tilde{N})}\,\mathrm{mod}\,\mathcal{LH}^0_1$, *where*
$\mathcal{LH}^0_1=\mathcal{L}^0(v_0)_{\mathcal{K}'}+t'^{q(b^*-a^*)}\sum_{1\leqslant j<p}t'^{-(j-1)a^*}C_j(\mathcal{L}_O)$.

This technical result from [3] can be translated into the covariant setting and the notation from this paper as follows.

Let $v_0=c_0$.

Consider the map Π from $\mathcal{L}^0$ to $\mathcal{L}$ such that $\Pi_k(\mathcal{D}_{an})=D_{an}$ 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 (ramification) ideal $\mathcal{L}^0(v_0)$ is mapped to $\mathcal{L}^{(c_0)}$. Essentially, Π is a morphism of Lie algebras (where $\mathcal{L}^0$ is taken with the opposite Lie structure) and it induces isomorphism of the appropriate quotients by $\mathcal{L}^0(c_0)$ and $\mathcal{L}^{(c_0)}$, respectively (use that by Proposition 2.1 all $D_{an}\in\mathcal{L}^{(c_0)}_k$ if $a>(p-1)c_0$).

Clearly, $\Pi_{\mathcal{K}'}(\hat{e}^{(0)}_{\mathcal{L}})\equiv e\,\mathrm{mod}\,\mathcal{L}^{(c_0)}_{\mathcal{K}'}$ and

$$\Pi_{\mathcal{K}'}(e'_{\mathcal{L}})\equiv e':=\sum_{a\in\mathbb{Z}^0(p)}t'^{-a}D_{a,-N^*}\,\mathrm{mod}\,\mathcal{L}^{(c_0)}_{\mathcal{K}'}\,.$$

If $\phi_0:=\Pi_{\mathcal{K}'}(\phi_0^{(\tilde{N})})$ then $\phi_0\equiv(-\phi)\circ(\sigma^{N^*}\phi')\,\mathrm{mod}\,\mathcal{L}^{(c_0)}_{\mathcal{K}'}$, where we set $\phi=(\sigma^{\tilde{N}}e)\circ\dots\circ(\sigma e)\circ e$ and $\phi'=(\sigma^{\tilde{N}}e')\circ\dots\circ(\sigma e')\circ e'$.

Let

$$\mathcal{M}_{\mathcal{K}'}:=\sum_{1\leqslant j<p}t^{-c_0j}\mathcal{L}(j)_{\mathrm{m}'}+\mathcal{L}(p)_{\mathcal{K}'}\,,$$

where m' is the maximal ideal of the valuation ring O_0 of $\mathcal{K}'$. Similarly, set

$$\mathcal{M}_{\mathcal{K}'_{<p}}=\sum_{1\leqslant j<p}t^{-c_0j}\mathcal{L}(j)_{\mathrm{m}'_{<p}}+\mathcal{L}(p)_{\mathcal{K}'_{<p}}$$

where $\mathcal{K}'_{<p}$ and $\mathrm{m}'_{<p}$ are the analogs of $\mathcal{K}_{<p}$ and $\mathrm{m}_{<p}$ for $\mathcal{K}'$.

Note that the above introduced modules $\mathcal{M}_{\mathcal{K}'}$ and $\mathcal{M}_{\mathcal{K}'_{<p}}$ are not obtained from $\mathcal{M}$ and, resp., $\mathcal{M}_{<p}$ when we replace $\mathcal{K}$ by $\mathcal{K}'$. Under

such replacement we obtain from $\mathcal{M}$ and $\mathcal{M}_{<p}$ the following modules

$$\mathcal{M}' := \sum_{1\leqslant j<p} t'^{\,-c_0j}\mathcal{L}(j)_{\mathrm{m}'} + \mathcal{L}(p)_{\mathcal{K}'}\,,$$

$$\mathcal{M}'_{<p} := \sum_{1\leqslant j<p} t'^{\,-c_0j}\mathcal{L}(j)_{\mathrm{m}'_{<p}} + \mathcal{L}(p)_{\mathcal{K}'_{<p}}\,.$$

However, $\sigma^{N^*}\mathcal{M}'\subset\mathcal{M}_{\mathcal{K}'}$ and $\sigma^{N^*}\mathcal{M}'_{<p}\subset\mathcal{M}_{\mathcal{K}'_{<p}}$.

Now we use the special choice of involved parameters to deduce from above Proposition 2.5 the following proposition.

Proposition 2.6. a) $\phi_0, \sigma(\phi_0)\in\mathcal{M}_{\mathcal{K}'}+\mathcal{L}^{(c_0)}_{\mathcal{K}'}$;

b) $e\circ\phi_0\equiv(\sigma\phi_0)\circ(\sigma^{N^*}e')\,\mathrm{mod}\,\left(t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'}+\mathcal{L}^{(c_0)}_{\mathcal{K}'}\right)$

Proof. a) From the definition of a^* it follows that $a^*=(c_0-\delta)q<c_0q$. Therefore, for $1\leqslant j<p$,

$$t'^{\,-ja^*}\Pi(C_j(\mathcal{L}_O))\subset t'^{\,-ja^*}O_0C_j(\mathcal{L})\subset t^{-jc_0}\mathrm{m}'C_j(\mathcal{L})\subset t^{-jc_0}\mathcal{L}(j)_{\mathrm{m}'}\,.$$

For part b), we need for $1\leqslant j<p$,

$$q(b^*-a^*)-(j-1)a^*>(p-j-1)qc_0\,.$$

This can be rewritten as $q(r^*-(c_0-\delta))>r^*+(p-2)c_0-(j-1)\delta$. This follows from the inequality $p\delta<2v_0$ in a) and the first inequality in d) from the beginning of this subsection. □

2.4. **Implication a) ⇔ b), I.** Suppose $h_{<p}$ is arithmetical. This means that $h^{(c_0)}=h_{<p}|_{\mathcal{K}^{(c_0)}}=h(p)|_{\mathcal{K}^{(c_0)}}$ is (a unique) arithmetical lift of h. Then the appropriate $\bar{c}_1=c_1\,\mathrm{mod}(\mathcal{M}(p-1)+\mathcal{L}^{(c_0)}_{\mathcal{K}_{<p}})$ appears as the "linear part of c" if and only if

$$(\mathrm{id}_{\bar{\mathcal{L}}}\otimes h(p)^U)\bar{f}=c_1U\circ f\,\mathrm{mod}\,(\mathcal{M}_{<p}U^2+t^{c_0(p-1)}\mathcal{M}_{<p}U+\mathcal{L}^{(c_0)}_{\mathcal{K}_{<p}}U)\,.$$

Consider the field $\mathcal{K}'$ from Subsection 2.3. This field is isomorphic to $\mathcal{K}$ and this isomorphism can be extended to an isomorphism of $\mathcal{K}_{<p}$ and its analog $\mathcal{K}'_{<p}$. Let $f'\in\mathcal{M}'_{<p}$ be such that $\sigma f'=e'\circ f'$. Then Proposition 2.6 b) implies the following lemma.

Lemma 2.7. *f' can be chosen in such a way that*

$$f\equiv\phi_0\circ\sigma^{N^*}f'\,\mathrm{mod}\,\left(t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'_{<p}}+\mathcal{L}^{(c_0)}_{\mathcal{K}'_{<p}}\right)\,.$$

Proof. Let $g=(-f)\circ\phi_0\circ\sigma^{N^*}f'\in\mathcal{M}'_{\mathcal{K}'_{<p}}$. Then by Proposition 2.6b)

$$\sigma g\equiv g\,\mathrm{mod}\,(t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'_{<p}}+\mathcal{L}^{(c_0)}_{\mathcal{K}'_{<p}})\,.$$

This congruence implies that

$$g\in\mathcal{L}+t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'_{<p}}+\mathcal{L}^{(c_0)}_{\mathcal{K}'_{<p}}$$

(use that σ is topologically nilpotent on $t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'_{<p}} \operatorname{mod} \mathcal{L}(p)_{\mathcal{K}'_{<p}}$). Therefore, there is $l \in \mathcal{L}$ such that $g \equiv l \operatorname{mod} (t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}^{(c_0)}_{\mathcal{K}'_{<p}})$ and we obtain our lemma with f' replaced by $f' \circ (-l)$. $\square$

2.5. **Implication a) $\Leftrightarrow$ b), II.** Now note that $\mathcal{K} \subset \mathcal{K}'$ induces the embeddings $\mathcal{K}_{<p} \subset \mathcal{K}'\mathcal{K}_{<p} \subset \mathcal{K}'_{<p}$.

Suppose $g \in \mathcal{I}_{\mathcal{K}}$ and $\hat{g} \in \mathcal{I}$ is its arithmetical lift (i.e. for any finite field extension $\mathcal{E}/\mathcal{K}$, $v(\hat{g}|_{\mathcal{E}}) = \varphi^{-1}_{\mathcal{E}/\mathcal{K}}(v(g))$). Introduce (similarly to $\mathcal{M}_{\mathcal{K}'_{<p}}$)

$$\mathcal{M}_{R_0} = \sum_{1\leqslant j<p} t^{-c_0 j}\mathcal{L}(j)_{\mathrm{m}_R} + \mathcal{L}(p)_{R_0}\,.$$

Then Lemma 2.7 implies that modulo $t^{c_0(p-1)}\mathcal{M}_{R_0} + \mathcal{L}^{(c_0)}_{R_0}$ we have

$$(\mathrm{id}_{\mathcal{L}} \otimes g_{<p})f \equiv (-\mathrm{id}_{\mathcal{L}} \otimes g)\phi \circ (\mathrm{id}_{\mathcal{L}} \otimes g')\sigma^{N^*}\phi' \circ (\mathrm{id}_{\mathcal{L}} \otimes g'_{<p})\sigma^{N^*} f'\,.$$

Here $g_{<p} := \hat{g}|_{\mathcal{K}_{<p}}$, $g'_{<p} := \hat{g}|_{\mathcal{K}'_{<p}}$ and $g' := \hat{g}|_{\mathcal{K}'}$ are all arithmetical over $\mathcal{K}$. (Recall, $\phi_0 \equiv (-\phi) \circ (\sigma^{N^*}\phi')$, cf. Section 2.4.)

Proposition 2.8. *Suppose $v(g) = c_0$. Then*

a) $(\mathrm{id}_{\mathcal{L}} \otimes g'_{<p} - \mathrm{id}_{\mathcal{K}'_{<p}})\sigma^{N^*} f' \in t^{c_0(p-1)}\mathcal{M}_{R_0}$;

b) $(\mathrm{id}_{\mathcal{L}} \otimes g' - \mathrm{id}_{\mathcal{K}'})\sigma^{N^*}\phi' \in t^{c_0(p-1)}\mathcal{M}_{R_0}$.

Proof. Let $\mathcal{K}'(p)$ be an analogue of $\mathcal{K}(p)$ for $\mathcal{K}'$.
If we set $g'_{(p)} = \hat{g}|_{\mathcal{K}'(p)}$ then it is arithmetical over $\mathcal{K}$ and

$$v(g'_{(p)}) = \varphi^{-1}_{(p)}(\varphi^{-1}_{\mathcal{K}'/\mathcal{K}}(c_0)) = \varphi^{-1}_{(p)}(r^* + q(c_0 - r^*)) > e_{(p)}c_0(p-1)\,,$$

cf. item d) in Section 2.3. This means that for any $a \in \mathcal{K}'(p)$,

$$g'_{(p)}(a) - a \in at'^{c_0(p-1)}R\,. \tag{2.3}$$

Now notice that $f' \operatorname{mod} \mathcal{L}(p)_{\mathcal{K}'_{<p}} \in \bar{\mathcal{L}}_{\mathcal{K}'(p)}$, cf. [6], Section 1.3. This implies that $f' \in \mathcal{M}_{\mathcal{K}'(p)} + \mathcal{L}(p)_{\mathcal{K}'_{<p}}$, where $\mathcal{M}_{\mathcal{K}'(p)}$ is an analogue of $\mathcal{M}_{\mathcal{K}'_{<p}}$ for $\mathcal{K}'(p)$. Now property (2.3) implies that

$$(\mathrm{id}_{\mathcal{L}} \otimes g'_{<p})f' - f' \in t'^{c_0(p-1)}\mathcal{M}'_{R_0} + \mathcal{L}(p)_{R_0} = t'^{c_0(p-1)}\mathcal{M}'_{R_0}\,,$$

where $\mathcal{M}'_{R_0} := \sum_{1\leqslant j<p} t'^{-c_0 j}\mathcal{L}(j)_{\mathrm{m}_R} + \mathcal{L}(p)_{R_0}$, and we obtain a) by applying σ^{N^*}.

For similar reasons,

$$v(g') = r^* + q(c_0 - r^*) > \varphi_{(p)}(e_{(p)}c_0(p-1)) \geqslant c_0(p-1)$$

(we use that $\varphi_{(p)}(e_{(p)}x) \geqslant x$ for any $x \geqslant 0$), and then for any $a \in \mathcal{K}'$,

$$g'(a) - a \in at'^{c_0(p-1)}R\,.$$

This implies

$$(\mathrm{id}_{\mathcal{L}} \otimes g')e' - e' \in t'^{c_0(p-1)}\mathcal{M}'_{R_0}\,,\quad (\mathrm{id}_{\mathcal{L}} \otimes g')\phi' - \phi' \in t'^{c_0(p-1)}\mathcal{M}'_{R_0}\,,$$

and we obtain b) by applying σ^{N^*}. $\square$

Corollary 2.9. *Suppose $g\in\mathcal{I}_{\mathcal{K}}$, $v(g)=c_0$ and $g_{<p}$ is a lift of g to $\mathcal{K}_{<p}$. Then the following conditions are equivalent:*

a) *$g_{<p}$ is arithmetical lift of g;*

b) $(\mathrm{id}_{\mathcal{L}}\otimes g_{<p})f\equiv(-\mathrm{id}_{\mathcal{L}}\otimes g)\phi\circ\phi\circ f\,\mathrm{mod}\,(t^{c_0(p-1)}\mathcal{M}_{R_0}+\mathcal{L}^{(c_0)}_{R_0})$.

Proof. Assume that $g_{<p}$ is arithmetical. We can assume that $g_{<p}=g'_{<p}|_{\mathcal{K}_{<p}}$ where $g'_{<p}\in\mathcal{I}_{\mathcal{K}'_{<p}}$ is arithmetical lift of g. Then Lemma 2.7 and Proposition 2.8 imply that modulo $t^{c_0(p-1)}\mathcal{M}_{R_0}+\mathcal{L}^{(c_0)}_{R_0}$

$$(\mathrm{id}_{\mathcal{L}}\otimes g_{<p})f\equiv(-\mathrm{id}_{\mathcal{L}}\otimes g)\phi\circ(\mathrm{id}_{\mathcal{L}}\otimes g')\sigma^{N^*}\phi'\circ(\mathrm{id}_{\mathcal{L}}\otimes g'_{<p})\sigma^{N^*}f'$$

$$\equiv(-\mathrm{id}_{\mathcal{L}}\otimes g)\phi\circ\phi\circ\phi_0\circ\sigma^{N^*}f'\equiv(-\mathrm{id}_{\mathcal{L}}\otimes g)\phi\circ\phi\circ f\,,$$

and we obtained b).

Assume that b) holds. If $g^o_{<p}\in\mathcal{I}_{\mathcal{K}_{<p}}$ is an arithmetical lift of g then we can apply b) and obtain

$$(\mathrm{id}_{\mathcal{L}}\otimes g_{<p})f\equiv(\mathrm{id}_{\mathcal{L}}\otimes g^o_{<p})f\,\mathrm{mod}\,(t^{c_0(p-1)}\mathcal{M}_{R_0}+\mathcal{L}^{(c_0)}_{R_0})\,.$$

On the other hand, there is $l\in G(\mathcal{L})$ such that $g_{<p}=g^o_{<p}\eta_0^{-1}(l)$. Then the above congruence implies that

$$l\in t^{c_0(p-1)}\mathcal{M}_{R_0}+\mathcal{L}^{(c_0)}_{R_0}\subset\mathrm{m}_R\mathcal{L}_R+\mathcal{L}^{(c_0)}_{R_0}\,.$$

But then $l\in\left(\mathrm{m}_R\mathcal{L}_R+\mathcal{L}^{(c_0)}_{R_0}\right)|_{\sigma=\mathrm{id}}=\mathcal{L}^{(c_0)}$. Therefore, $g_{<p}$ is also arithmetical. □

2.6. **Implication a) ⇔ b), III.** Let $1\leqslant n<p$. Applying Corollary 2.9 to $g=h^n$ and its lift $h^n_{<p}$ we obtain that the following two properties are equivalent:

- $h^n_{<p}$ is arithmetical;
- $(\mathrm{id}_{\mathcal{L}}\otimes h^n_{<p})f=c(n)\circ(A^n\otimes\mathrm{id}_{\mathcal{K}_{<p}})f$, where $(A^n-\mathrm{id}_{\mathcal{L}})\mathcal{L}\subset\mathcal{L}^{(c_0)}$

and $c(n)\equiv(-\mathrm{id}_{\mathcal{L}}\otimes h^n)\phi\circ\phi\,\mathrm{mod}\,\mathcal{M}(p-1)+\mathcal{L}^{(c_0)}_{\mathcal{K}}$.

Clearly, the first condition holds if and only if $h_{<p}$ is arithmetical.

The second condition means that $(A-\mathrm{id}_{\mathcal{L}})\mathcal{L}\subset\mathcal{L}^{(c_0)}$ and

$$c(U)\equiv(-\mathrm{id}_{\mathcal{L}}\otimes h^U)\phi\circ\phi\,\mathrm{mod}\,\mathcal{M}(p-1)+\mathcal{L}^{(c_0)}_{\mathcal{K}}\,.$$

The both parts of the last congruence can be recovered uniquely from their linear terms: this is obvious for $(-\mathrm{id}_{\mathcal{L}}\otimes h^U)\phi\circ\phi$ and was explained in [6], Section 3.5, for $c(U)$, cf. also overview in Section 2.1. Therefore, the equivalence of a) and b) will be proved if we show that the linear part of $(-\mathrm{id}_{\mathcal{L}}\otimes h^U)\phi\circ\phi$ takes the prescribed value from part b) of our theorem.

Recall that $\phi=(\sigma^{\tilde{N}}e)\circ\cdots\circ(\sigma e)\circ e$.

Apply identities (3.5) and (3.6) from Subsection 3.2 of [6], use the definition of the elements $\mathcal{F}^0_{\gamma,-N}\in\mathcal{L}_k$ from Subsection 1.4 of [6] and the abbreviation $d_h := d(\mathrm{id}_{\mathcal{L}} \otimes h^U)$ to obtain the following congruences modulo U^2:

$$e + d_h e \equiv e \circ \left(\sum_{k \geqslant 1} (1/k!)[\dots[d_h e, \underbrace{e], \dots, e]}_{k-1 \text{ times}} \right)$$

$$\equiv e \circ \left(-U \sum_{\gamma > 0\,, j \geqslant 0} A_j(h) \mathcal{F}^0_{\gamma,0}\, t^{-\gamma + c_0 + pj} \right)$$

Similarly,

$$\sigma e + \sigma d_h e \equiv \sigma e \circ \left(\sum_{k \geqslant 1} (1/k!)[\dots[\sigma d_h e, \underbrace{\sigma e], \dots, \sigma e]}_{k-1 \text{ times}} \right)$$

then

$$(\sigma e + \sigma d_h e) \circ e \equiv$$

$$(\sigma e) \circ e \circ \left(\sum_{\substack{k_0 \geqslant 1 \\ k_1 \geqslant 0}} \frac{1}{k_0! k_1!} [\dots[\sigma d_h e, \underbrace{\sigma e], \dots, \sigma e]}_{k_0 - 1 \text{ times}}, \underbrace{e], \dots, e]}_{k_1 \text{ times}} \right)$$

$$= (\sigma e) \circ e \circ \left(-U \sum_{\substack{\gamma > 0 \\ j \geqslant 0}} \sigma(A_j(h) \mathcal{F}^0_{\gamma,-1} t^{-\gamma + c_0 + pj}) \right)$$

and taking above formulas together we obtain $\eta_0(\tau) = (-f) \circ \tau(f)$

$$(\sigma e + \sigma d_h e) \circ (e + d_h e) \equiv (\sigma e) \circ e \circ \left(-U \sum_{\substack{\gamma > 0 \\ j \geqslant 0}} \sum_{0 \leqslant i \leqslant 1} \sigma^i (A_j(h) \mathcal{F}^0_{\gamma,-i} t^{-\gamma + c_0 + pj}) \right)$$

We can continue similarly to obtain that

$$(\mathrm{id} \otimes h^U)\phi \equiv \phi \circ \left(-U \sum_{\substack{\gamma > 0 \\ j \geqslant 0}} \sum_{0 \leqslant i \leqslant \widetilde{N}} \sigma^i (A_j(h) \mathcal{F}^0_{\gamma,-i} t^{-\gamma + c_0 + pj}) \right) \bmod U^2$$

$\eta_0(\tau) = (-f) \circ \tau(f)$

So, the linear term takes the prescribed value and the statements a) and b) of theorem are equivalent.

2.7. **The end of proof of Theorem 2.4.** Obviously, b) implies c).

Suppose a lift $h_{<p}$ has ingredients c_1 and $\{V_{a0}\mid a\in\mathbb{Z}^0(p)\}$ and $c_1(0)$ satisfies the condition c) of our theorem. Take the maximal $1\leqslant s_0\leqslant p$ such that $h_{<p}|_{\mathcal{K}_{<p}^{G(\mathcal{L}(s_0))}}$ is arithmetical. If $s_0=p$ then $h(p)$ is arithmetical and this implies that $h_{<p}$ is arithmetical.

Suppose $s_0<p$.

Let $h^o_{<p}$ be some arithmetical lift of h with the appropriate ingredients c_1^o and $\{V_a^o\mid a\in\mathbb{Z}^0(p)\}$. Therefore,

$$c_1\equiv c_1^o \operatorname{mod}\mathcal{L}_{\mathcal{K}}^{(c_0)}+\mathcal{L}(s_0)_{\mathcal{K}}\,.$$

Note that for all $a\in\mathbb{Z}^0(p)$, $V_{a0}\in\mathcal{L}_k^{(c_0)}+\mathcal{L}(s_0)_k$ and $V_a^o\in\mathcal{L}_k^{(c_0)}$. Then recurrent relation (2.2) (considered at the s_0-th step) implies that

$$\sigma c_1-c_1+\sum_{a\in\mathbb{Z}^0(p)}t^{-a}V_{a0}\equiv\sigma c_1^o-c_1^o\operatorname{mod}\mathcal{L}_{\mathcal{K}}^{(c_0)}+\mathcal{L}(s_0+1)_{\mathcal{K}}\,.$$

Therefore, by [6], Lemma 2.2b), all $V_{a0}\in\mathcal{L}_k^{(c_0)}+\mathcal{L}(s_0+1)_k$ and

$$c_1-c_1^o\equiv c_1(0)-c_1^o(0)\operatorname{mod}\mathcal{L}_{\mathcal{K}}^{(c_0)}+\mathcal{L}(s_0+1)_{\mathcal{K}}\,.$$

So, if $c_1(0)$ satisfies c) then $c_1\equiv c_1^o\operatorname{mod}\mathcal{L}_{\mathcal{K}}^{(c_0)}+\mathcal{L}(s_0+1)_{\mathcal{K}}$ and the restriction $h_{<p}|_{\mathcal{K}_{<p}^{G(\mathcal{L}(s_0+1))}}$ is arithmetical. The contradiction. Theorem 2.4 is completely proved.

3. Explicit calculations in L_h

In this Section we apply the above techniques to study the lifts $h(p)=h_{<p}|_{\mathcal{K}(p)}$. In Section 2 we studied the properties of $h_{<p}|_{\mathcal{K}^{(c_0)}}$ and that was sufficient to characterize arithmetical lifts $h_{<p}$. If we want to describe the structure of the Lie algebra L_h we need to study the invariants $\operatorname{ad}h(p)$ and c_1 of $h(p)$.

Suppose $h(p)$ is given, as earlier, via

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

with the appropriate $\bar c\in\mathcal{M}\operatorname{mod}\mathcal{M}(p-1)$. Then the relevant elements $c_1\in\mathcal{L}_{\mathcal{K}}\operatorname{mod}\mathcal{M}(p-1)$ and $V_{a0}=\mathrm{ad}h(p)(D_{a0})\in\bar{\mathcal{L}}_k=\mathcal{L}_k/\mathcal{L}(p)_k$, $a\in\mathbb{Z}^0(p)$, satisfy recurrent relation (2.2). This allows us to proceed from solutions $(c_1,\sum_a t^{-a}V_{a0})$ obtained modulo $\mathcal{M}(p-1)+\mathcal{L}(s)_{\mathcal{K}}$ to the appropriate "more precise" solutions modulo $\mathcal{M}(p-1)+\mathcal{L}(s+1)_{\mathcal{K}}$, for all $1\leqslant s<p$.

As earlier, let $c_1=\sum_{m\in\mathbb{Z}}c_1(m)t^m$, where all $c_1(m)\in\bar{\mathcal{L}}_k$. 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 find "precise" formulas for c^+, $c(0)$ and $V_0=\alpha_0^{-1}V_{00}=\mathrm{ad}h(p)(D_0)$. The expression for $\mathrm{ad}h(p)(D_0)$ is given in Proposition 3.4 below.

It would be very interesting to resolve completely recurrent relation (2.2) and to find reasonably compact formulas for c_1^- and all the elements $V_{a0} = \mathrm{ad}\, h(p)(D_{a0})$, $a \in \mathbb{Z}^+(p)$. This would generalize explicit calculations from [6], Subsection 3.6. Some steps in this direction have been made recently by K. McCabe (PhD Thesis, Durham University).

3.1. **Explicit formula for c_1^+.** Consider all $(\bar{a}, \bar{n}) = (a_1, n_1, \dots, a_s, n_s)$ such that $1 \leqslant s < p$, all $a_i \in \mathbb{Z}^0(p)$ and $n_1 \geqslant n_2 \geqslant \dots \geqslant n_s = 0$.

Set $\gamma(\bar{a}, \bar{n}) = a_1 p^{n_1} + a_2 p^{n_2} + \dots + a_s p^{n_s}$.

Set $D_{(\bar{a},\bar{n})} := [\dots[D_{a_1 n_1}, D_{a_2 n_2}], \dots, D_{a_s n_s}]$ and $\mathrm{wt} D_{(\bar{a},\bar{n})} := s_1 + \dots + s_n$, where for all $1 \leqslant i \leqslant n$, $(s_i - 1)c_0 \leqslant a_i < s_i c_0$.

Denote by $\delta^+(c_0)$ the minimum of all positive values of

$$(c_0 + pj) - p^{-n_1}\gamma(\bar{a}, \bar{n}),$$

where $j \geqslant 0$ and $(\bar{a}, \bar{n})$ runs over the set of all above vectors with additional condition $\mathrm{wt} D_{(\bar{a},\bar{n})} < p$.

Finally, let $N^+(c_0) = \min\{n \geqslant 0 \mid p^n \delta^+(c_0) \geqslant c_0(p-1)\}$.

Relation (2.2) implies that modulo $\mathcal{M}(p-1)$

$$\sigma c_1^+ - c_1^+ \equiv \tag{3.1}$$

$$-\sum_{\substack{k \geqslant 1 \\ j \geqslant 0}} \frac{1}{k!} A_j(h) \sum_{a_1, \dots, a_k} t^{c_0 + pj - (a_1 + \dots + a_k)} [\dots[a_1 D_{a_1 0}, D_{a_2 0}], \dots, D_{a_k 0}]$$

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

In both above sums the indices $a_1, \dots, a_k$ run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \dots + a_k < c_0 + pj$ for the first sum and $a_1 + \dots + a_k < pm$ for the second sum.

Note that $c_1^+ \bmod \mathcal{M}(p-1)$ is defined uniquely by (3.1).

Definition. For $n^* \geqslant n_*$, let $\mathcal{F}^0_{\gamma,[n^*,n_*]}$ be the partial sum of $\sigma^{n^*} \mathcal{F}^0_{\gamma, n_* - n^*}$ containing only the terms $[\dots[D_{a_1 n_1}, D_{a_2 n_2}], \dots, D_{a_s n_s}]$, such that $n_1 = n^*$ and $n_s = n_*$. In other words, we keep only the terms such that $n^* = \max\{n_i \mid 1 \leqslant i \leqslant s\}$ and $n_* = \min\{n_i \mid 1 \leqslant i \leqslant s\}$.

Proposition 3.1. *Let $N^0 \in \mathbb{N}$ be such that $N^0 \geqslant N^+(c_0) - 1$. Then*

$$c_1^+ \equiv \sum_{\substack{j \geqslant 0 \\ 0 \leqslant n \leqslant N^0}} \sum_{\gamma < c_0 + pj} \sigma^n (A_j(h) \mathcal{F}^0_{\gamma, -n}) t^{p^n (c_0 + pj - \gamma)} \bmod \mathcal{M}(p-1).$$

Remark. The RHS of the above congruence does not depend on a choice of $N^0 \geqslant N^+(c_0) - 1$.

Proof of Proposition. Prove proposition by establishing the formula for c_1^+ modulo $\mathcal{M}(p-1) + C_s(\mathcal{L}_{\mathcal{K}})$ by induction on $1 \leqslant s \leqslant p$.

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

Suppose $s<p$ and proposition is proved modulo $\mathcal{M}(p-1)+C_s(\mathcal{L}_{\mathcal{K}})$. Prove that modulo $\mathcal{M}(p-1)+C_{s+1}(\mathcal{L}_{\mathcal{K}})$

$$\sigma c_1^+ - c_1^+ \equiv -\sum_{\substack{j\geqslant 0\\ 0\leqslant n\leqslant N^0}} \sigma^n(A_j(h)) \sum_{\gamma<c_0+pj} \mathcal{F}^0_{\gamma,[n,0]} t^{p^n(c_0+pj-\gamma)}\,. \tag{3.2}$$

Note that for $n=0$,

$$\mathcal{F}^0_{\gamma,[0,0]} = \sum_{a_1,\dots,a_k} \frac{1}{k!}[\dots[a_1D_{a_10},D_{a_20}],\dots,D_{a_k0}]$$

and for $n>0$,

$$\mathcal{F}^0_{\gamma,[n,0]} = \sum_{\substack{k\geqslant 1,\gamma'>0\\ a_1,\dots,a_k}} \frac{1}{k!}[\dots[\sigma^n\mathcal{F}^0_{\gamma',-(n-1)},D_{a_10}],\dots,D_{a_k0}]\,.$$

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

The first formula allows us to identify the first line of the RHS in (3.1) with the part of (3.2) which corresponds to $n=0$. The second formula allows us to rewrite modulo $C_{s+1}(\mathcal{L}_{\mathcal{K}})$ the second line of the RHS in (3.1) (under inductive assumption) as the part of (3.2) which corresponds to $n>0$.

Denote by $-\Omega$ the right-hand side of (3.2). Then we have modulo $\mathcal{M}(p-1)+C_{s+1}(\mathcal{L}_{\mathcal{K}})$ that $c_1^+\equiv\sum_{m\geqslant 0}\sigma^m\Omega$ and

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

Modulo $\mathcal{M}(p-1)$ we can assume that $n_1=n+m\leqslant N^0$ and rewrite the above RHS as

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

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

The proposition is proved. □

3.2. **Explicit calculations with** $c_1(0)$**.** By (2.2) we have modulo $\mathcal{L}(p)_k$ that (here $V_0=\alpha_0^{-1}V_{00}=\mathrm{ad}h(p)(D_0)$)

$$\begin{aligned}\sigma c_1(0)-c_1(0)+\alpha_0V_0 \equiv\\ -\sum_{\substack{k\geqslant 1\\ j\geqslant 0}}\sum_{a_1,\dots,a_k}\frac{1}{k!}A_j(h)[\dots[a_1D_{a_10},D_{a_20}],\dots,D_{a_k0}]\\ -\sum_{\substack{k,m\geqslant 1\\ a_1,\dots,a_k}}\frac{1}{k!}[\dots[\sigma c_1^+(m),D_{a_10}],\dots,D_{a_k0}]\end{aligned} \tag{3.3}$$

$$-\sum_{k\geqslant 2}\frac{1}{k!}[\dots[V_0,\underbrace{D_{00}],\dots,D_{00}]}_{k-1\text{ times}}$$

$$-\sum_{k\geqslant 1}\frac{1}{k!}[\dots[\sigma c_1(0),\underbrace{D_{00}],\dots,D_{00}]}_{k\text{ times}}$$

In the first and second sums the indices a_i run over $\mathbb{Z}^0(p)$ with the restrictions $a_1+\dots+a_k=c_0+pj$ in the first case and $a_1+\dots+a_k=pm$ in the second case.

Definition. For $n\geqslant 0$, denote by $\mathcal{F}^+_{\gamma,[n,0]}$ the partial sum of $\mathcal{F}^0_{\gamma,[n,0]}$ which contains only the terms with $[\dots[D_{a_1n_1},D_{a_2n_2}],\dots,D_{a_sn_s}]$ such that if for some $i_1\geqslant 0$, $0=n_s=\dots=n_{s-i_1}<n_{s-i_1-1}$ then at least one of $a_s,\dots,a_{s-i_1}$ is not zero.

Fix $N^0\geqslant N^+(c_0)-1$.

Lemma 3.2. *The sum of the first two lines in the RHS of* (3.3) *equals*

$$-\sum_{\substack{0\leqslant n\leqslant N^0\\ j\geqslant 0}}\sigma^n(A_j(h))\mathcal{F}^+_{c_0+pj,[n,0]}$$

Proof. For the first line use the above definition with $n=0$.

For the second line use the following identity

$$\sum_{\substack{k\geqslant 1\\ a_1,\dots,a_k}}(1/k!)[\dots[\sigma^n\mathcal{F}^0_{\gamma,-n+1},D_{a_10}],\dots,D_{a_k0}]=\mathcal{F}^+_{c_0+pj,[n,0]}$$

where $n\in\mathbb{N}$, $\gamma<c_0+pj$ and $a_1,\dots,a_k$ run over $\mathbb{Z}^0(p)$ such that $a_1+\dots+a_k=p^n(c_0+pj-\gamma)$. □

Introduce the operators

$$G_0=\widetilde{\exp}\,(\alpha_0\,\mathrm{ad}D_0),\quad F_0=E_0(\alpha_0\,\mathrm{ad}D_0)$$

on $\mathcal{L}_k$ (recall that $E_0(x)=(\widetilde{\exp}x-1)/x$). Note that for $l\in\mathcal{L}_k$,

$$F_0(l)=\sum_{k\geqslant 1}\frac{\alpha_0^{k-1}}{k!}[\dots[l,\underbrace{D_0],\dots,D_0]}_{k-1\text{ times}},\ \ G_0(l)=\sum_{k\geqslant 0}\frac{\alpha_0^{k}}{k!}[\dots[l,\underbrace{D_0],\dots,D_0]}_{k\text{ times}}.$$

With this notation we can rewrite (3.3) in the following form

$$(G_0\sigma-\mathrm{id})c_1(0)+F_0(\alpha_0V_0)=-\sum_{j\geqslant 0}\sum_{0\leqslant i\leqslant N^0}\sigma^i(A_j(h))\mathcal{F}^+_{c_0+pj,[i,0]}$$

Lemma 3.3. *Suppose* $l(\alpha,\gamma)=\sum_{0\leqslant i\leqslant N^0}\sigma^i(\alpha\mathcal{F}^0_{\gamma,-i})$*, where* $\alpha\in k$*. Then*

$$(G_0\sigma-\mathrm{id})l(\alpha,\gamma)=-\sum_{0\leqslant i\leqslant N^0}\sigma^i(\alpha)\mathcal{F}^+_{\gamma,[i,0]}+G_0\sigma^{N^0+1}(\alpha\mathcal{F}^0_{\gamma,-N^0})$$

Proof of lemma. Directly from definitions it follows for $i \geqslant 0$, that $(G_0\sigma)(\sigma^i\mathcal{F}^0_{\gamma,-i}) = \sigma^{i+1}\mathcal{F}^0_{\gamma,-(i+1)} - \mathcal{F}^+_{\gamma,[i+1,0]}$. Therefore,

$$(G_0\sigma)l(\alpha,\gamma) = \sum_{1\leqslant i\leqslant N^0+1}\sigma^i(\alpha\mathcal{F}^0_{\gamma,-i}) - \sum_{1\leqslant i\leqslant N^0+1}(\sigma^i\alpha)\mathcal{F}^+_{\gamma,[i,0]}$$

$$= l(\alpha,\gamma) - \sum_{0\leqslant i\leqslant N^0}(\sigma^i\alpha)\mathcal{F}^+_{\gamma,[i,0]} + \sigma^{N^0+1}(\alpha)\left(-\mathcal{F}^+_{\gamma,[N^0+1,0]} + \sigma^{N^0+1}\mathcal{F}^0_{\gamma,-(N^0+1)}\right).$$

It remains to note that $-\mathcal{F}^+_{\gamma,[N^0+1,0]} + \sigma^{N^0+1}\mathcal{F}^0_{\gamma,-(N^0+1)} = G_0\sigma^{N^0+1}\mathcal{F}^0_{\gamma,-N^0}$. □

Summarize the above calculations.

Proposition 3.4. *Suppose $h(p)$ is a lift of h to $\mathcal{K}(p)$ with the "linear ingredient" $c_1 = c_1^- + c(0) + c_1^+$, $V_0 = (\mathrm{ad}\, h(p))D_0$ and $N^0 \geqslant N^+(c_0) - 1$. Then*

$$c_1(0) = c^0 + \sum_{\substack{0\leqslant i\leqslant N^0\\ j\geqslant 0}}\sigma^i(A_j(h)\mathcal{F}^0_{c_0+pj,-i}) \in \bar{\mathcal{L}}_k\,,$$

where $c^0 \in \bar{\mathcal{L}}_k$ and $V_0 \in \bar{\mathcal{L}}$ are arbitrary solutions of the equation

$$(G_0\sigma - \mathrm{id})c^0 + F_0(\alpha_0 V_0) = -G_0\sigma^{N^0+1}\Omega^0\,, \tag{3.4}$$

with $\Omega^0 = \sum_{j\geqslant 0} A_j(h)\mathcal{F}^0_{c_0+pj,-N^0}$.

Remark. a) Modulo $[\bar{\mathcal{L}}_k, D_0]$ equation (3.4) looks like

$$(\sigma - \mathrm{id})c^0 + \alpha_0 V_0 \equiv -\sigma^{N^0+1}\Omega^0\,,$$

and, therefore, admits explicit solutions (use the operators $\mathcal{R}$ and $\mathcal{S}$ from [6], Subsection 2.2 together with Lemma 2.2b). This implies $V_0 = \mathrm{ad}\, h(p)(D_0)$ is congruent modulo $[\mathcal{L}_k, D_0]$ to (recall that $|k| = p^{N_0}$)

$$-(\mathrm{id}_{\mathcal{L}}\otimes \mathrm{Tr}_{k/\mathbb{F}_p})(\sigma^{N^0+1}\Omega^0) \equiv -\sum_{0\leqslant n<N_0}\sigma^n(\Omega^0);$$

b) if $k = \mathbb{F}_p$ then (3.4) can be solved: here $\sigma = \mathrm{id}$ and we can set $c^0 = -\Omega^0 (= -\sigma^{N^0}\Omega^0)$; this implies the existence of a lift $h(p)$ such that the Demushkin relation appears in the form

$$\mathrm{ad} h(p)(D_0) + F_0^{-1}(\Omega^0) = 0\,;$$

c) the appearance of operators F_0 and G_0 in the LHS of (3.4) is related to a "bad influence" of the generators D_{0n}; this influence can be seen already at the explicit expressions of the elements $\mathcal{F}^0_{\gamma,-N}$: the factors D_{0n} don't contribute to γ and therefore can appear with almost no restrictions in all terms of $\mathcal{F}^0_{\gamma,-N}$; e.g. if $a \in \mathbb{Z}^0(p)$ then $\mathcal{F}^0_{a,-N}$ contains together with the linear term aD_{a0} all terms from $(\sigma^{-N}G_0)(\sigma^{-N+1}G_0)\dots(\sigma^{-1}G_0)F_0(aD_{a0})$.

Finally note that Proposition 3.4 allows us to control arithmetic lifts of h if we require also that $N^0 \geqslant \widetilde{N}(c_0)$.

Proposition 3.5. *Suppose* $N^0 \geqslant \max\{N^+(c_0)-1, \widetilde{N}(c_0)\}$. *Then* (3.4) *admits a solution* $c^0 \in \bar{\mathcal{L}}_k^{(c_0)}$ *and* $V_0 \in \bar{\mathcal{L}}^{(c_0)}$ *and the corresponding lift* $h(p)$ *is arithmetical.*

Proof. For $n \geqslant 1$, define the triples (X_n, Y_n, Z_n) by the following recurrent relations:

$$Z_1 = -G_0\sigma^{N^0+1}\Omega^0, \quad X_n = \mathcal{S}(Z_n), \quad Y_n = \alpha_0^{-1}\mathcal{R}(Z_n)$$

$$Z_{n+1} = -(G_0 - \mathrm{id})\sigma X_n - (F_0 - \mathrm{id})(\alpha_0 Y_n)\,.$$

Then is it easy to see that:

1) for all n, $Z_n, X_n \in (\mathrm{ad}^{n-1}D_0)\bar{\mathcal{L}}_k^{(c_0)}$ and $Y_n \in (\mathrm{ad}^{n-1}D_0)\bar{\mathcal{L}}^{(c_0)}$;

2) $c^0 = X_1 + \dots + X_{p-1}$ and $V_0 = Y_1 + \dots + Y_{p-1}$ satisfy (3.4).

Indeed, for any ideal $\mathcal{L}'$ in $\bar{\mathcal{L}}$ and $n \geqslant 1$, the operators $\mathcal{R}$ and $\mathcal{S}$ map $(\mathrm{ad}^{n-1}D_0)\mathcal{L}'_k$ to itself and the operators $G_0 - \mathrm{id}$ and $F_0 - \mathrm{id}$ map $(\mathrm{ad}^{n-1}D_0)\mathcal{L}'_k$ to $(\mathrm{ad}^{n}D_0)\mathcal{L}'_k$. This proves the first property.

As for the second property, proceed as follows:

$$\sum_{1\leqslant i<p}(G_0\sigma - \mathrm{id})X_i + \sum_{1\leqslant i<p}F_0(\alpha_0 Y_i)$$

$$= \sum_{1\leqslant i<p}(G_0 - \mathrm{id})\sigma X_i + \sum_{1\leqslant i<p}(F_0 - \mathrm{id})(\alpha_0 Y_i) + \sum_{1\leqslant i<p}((\sigma - \mathrm{id})X_i + \alpha_0 Y_i)$$

$$= -(Z_2 + \dots + Z_{p-1} + Z_p) + (Z_1 + Z_2 + \dots + Z_{p-1}) = Z_1\,.$$

Finally Theorem 2.4c) implies that the appropriate lift $h(p)$ is arithmetical. □

4. The mixed characteristic case

4.1. **The field-of-norms functor.** Recall the relation between the mixed and characteristic p cases given by the field-of-norms functor, cf. [6], Subsection 4.1.

Suppose $[K : \mathbb{Q}_p] < \infty$ with the residue field $k \simeq \mathbb{F}_{p^{N_0}}$ and the ramification index e_K. Let $\pi_0 \in K$ be a uniformizer and a primitive p-th root of unity $\zeta_1 \in K$. Set $\Gamma = \mathrm{Gal}(\bar{K}/K)$ and $\Gamma_{<p} := \Gamma/\Gamma^p C_p(\Gamma)$. For $n \in \mathbb{N}$, choose $\pi_n \in \bar{K}$ such that $\pi_n^p = \pi_{n-1}$, let $\widetilde{K} = \bigcup_{n\in\mathbb{N}} K(\pi_n)$ and $\Gamma_{\widetilde{K}} = \mathrm{Gal}(\bar{K}/\widetilde{K})$. Then $\Gamma_{\widetilde{K}} \subset \Gamma$ and we have the induced continuous group homomorphism $\iota : \Gamma_{\widetilde{K}} \longrightarrow \Gamma_{<p}$. We also have a projection $j : \Gamma_{<p} \longrightarrow \mathrm{Gal}(K(\pi_1)/K) = \langle\tau_0\rangle^{\mathbb{Z}/p}$, where $\tau_0(\pi_1) = \pi_1\zeta_1$, and the exact sequence $\Gamma_{\widetilde{K}} \xrightarrow{\iota} \Gamma_{<p} \xrightarrow{j} \langle\tau_0\rangle^{\mathbb{Z}/p} \longrightarrow 1$.

Let R be Fontaine's ring and $R_0 = \mathrm{Frac}R$. We have a natural embedding $k \subset R$, the element $t = (\pi_n \bmod p)_{n\geqslant 0} \in R$ and $\mathcal{K} = k((t))$ is a closed subfield of R_0. Then the field-of-norms functor X identifies $X(\widetilde{K})$ with $\mathcal{K}$ and R_0 with the completion of $\mathcal{K}_{sep}$. There is also an inclusion $\iota_K : \Gamma_K \longrightarrow \mathrm{Aut}\, R_0$ which induces identification of $\Gamma_{\widetilde{K}}$ with $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$. This identification is compatible with the ramification filtrations on Γ_K and $\mathcal{G}$. The simplest version of this compatibility states that if $v \geqslant 0$ and $v' = \varphi_{\widetilde{K}/K}(v)$, where $\varphi_{\widetilde{K}/K}$ is the Herbrand function of $\widetilde{K}/K$ then

$$\iota_K(\Gamma_{\widetilde{K}} \cap \Gamma_K^{(v')}) = \mathcal{G}^{(v)}\,. \tag{4.1}$$

As a matter of fact, there is a more general property

$$\iota_K(\Gamma_K) \cap \mathcal{I}_{/\mathcal{K}}^{(v)} = \iota_K\left(\Gamma_K^{(v')}\right)\,. \tag{4.2}$$

This was stated in [11], Subsection 3.3, in the case of Galois APF extensions but the proof works word-by-word in the non-Galois case.

The identification $\iota_K|_{\Gamma_{\widetilde{K}}}$ composed with ι induces a natural continuous morphism of groups $\iota_{<p} : \mathcal{G}_{<p} \longrightarrow \Gamma_{<p}$ and we obtain the exact sequence $\mathcal{G}_{<p} \xrightarrow{\iota_{<p}} \Gamma_{<p} \xrightarrow{j} \langle\tau_0\rangle^{\mathbb{Z}/p} \longrightarrow 1$.

4.2. **Isomorphism $\kappa_{<p}$.** Recall the construction of the group isomorphism $\kappa_{<p} : \Gamma_{<p} \longrightarrow \mathcal{G}_h$ from [6], Subsection 4.3.

Let η be a closed embedding of $\mathcal{K}$ into R_0 which is compatible with the extension $v_{\mathcal{K}}$ to R_0 of the normalized valuation of $\mathcal{K}$.

Let $c_0 := e^*(= e_K p/(p-1))$. We have $e \in \mathcal{M} \subset \mathcal{L}_{\mathcal{K}}$, $f \in \mathcal{M}_{<p} \subset \mathcal{L}_{\mathcal{K}_{<p}}$, and if $\hat{\eta} \in \mathrm{Aut} R_0$ is a lift of η then $(\mathrm{id}_{\mathcal{L}} \otimes \hat{\eta})f \in \mathcal{M}_{R_0} \subset \mathcal{L}_{R_0}$. By [6], Proposition 4.3 c), we have

Proposition 4.1. *Suppose* $(\mathrm{id}_{\mathcal{L}} \otimes \eta)e \equiv e \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$. *Then there is a unique lift* $\eta(p)$ *of* η *to* $\mathcal{K}(p)$ *such that* $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta(p))\bar{f} = \bar{f}$, *where* $\bar{f} = f \bmod t^{(p-1)c_0}\mathcal{M}_{R_0}$.

Let $\varepsilon = (\zeta_n \bmod p)_{n \geqslant 0} \in R$, where ζ_1 is our fixed p-th primitive root of unity. If $\zeta_1 = 1 + \pi_0^{c_0/p}\sum_{i \geqslant 0}[\beta_i]\pi_0^i$ where all $[\beta_i]$ are the Teichmuller representatives of $\beta_i \in k$ and $\beta_0 \neq 0$ then (note $\varepsilon \notin \mathcal{K}$)

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

Let $h \in \mathrm{Aut}\mathcal{K}$ be such that $h|_k = \mathrm{id}_k$ and $h(t) \equiv t\varepsilon \bmod t^{(p-1)c_0+1}R$. We can assume that $h(t) = t\widetilde{\exp}(\omega_h^p)$, where $\omega_h \in t^{c_0/p}k[[t]]^*$, i.e. h satisfies the conditions from the beginning of Section 2.1.

For any $\tau \in \Gamma$, there is $\tilde{h} \in \langle h\rangle \subset \mathrm{Aut}\,\mathcal{K}$ such that $\iota_K(\tau)|_{\mathcal{K}}(t) \equiv \tilde{h}(t) \bmod t^{(p-1)c_0+1}R$ and this $\tilde{h}$ is unique modulo $\langle h^p\rangle$. This means that $\eta := \iota_K(\tau)|_{\mathcal{K}}\tilde{h}^{-1} : \mathcal{K} \longrightarrow R_0$ satisfies the assumption from Proposition 4.1 amd we obtain a unique lift $\eta(p) \in \mathrm{Aut}\mathcal{K}(p)$ of η.

Then $\tilde{h}(p) := \eta(p)^{-1}\iota_K(\tau)|_{\mathcal{K}(p)} \in \operatorname{Aut}\mathcal{K}(p)$ and $\tilde{h}(p)|_{\mathcal{K}} = \tilde{h}$. 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

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

In addition, the image $\kappa(\tau)$ of $\tilde{h}(p)$ in $\mathcal{G}_h$ is well-defined.

As a result, the map $\kappa : \Gamma \longrightarrow \mathcal{G}_h$ is uniquely characterized by

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

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 $\kappa(\tau) \in \mathcal{G}_h$.

Proposition 4.2. *κ induces a group isomorphism $\kappa_{<p} : \Gamma_{<p} \longrightarrow \mathcal{G}_h$.*

For the proof cf. [6], Proposition 4.4.

4.3. **Ramification filtrations.** Recall that $\Gamma_{<p} = G(L)$ has the induced fitration by the images $\Gamma^{(v)}_{<p}$, $v \geqslant 0$, of the ramification subgroups $\Gamma^{(v)}$ with respect to the projection $\mathrm{pr}_{<p} : \Gamma \longrightarrow \Gamma_{<p}$. This gives the appropriate filtration by the ideals $L^{(v)}$ of the Lie algebra L.

As earlier in Section 4.2, the elements of $\iota_K(\Gamma) \subset \mathrm{Aut}R_0$ can be considered as the elements of the ramification subsets $\mathcal{I}^{(v)}_{/\mathcal{K}}$, $v \geqslant 0$. This gives the induced filtration $L^{(v)}_{/\mathcal{K}}$ on L (the notation indicates to the "upper numbering with respect to $\mathcal{K}$") such that $G(L^{(v)}_{/\mathcal{K}})$ is the image of $\iota_K^{-1}(\iota_K(\Gamma) \cap \mathcal{I}^{(v)}_{/\mathcal{K}})$ under the projection $\mathrm{pr}_{<p}$. By property (4.2) we have $L^{(v)}_{/\mathcal{K}} = L^{(\varphi_{\tilde{K}/K}(v))}$.

The elements of $\mathcal{G}_h = G(L_h)$ are related to the field automorphisms $\mathrm{Aut}\mathcal{K}(p)$ via the natural projection of $\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h) \subset \mathrm{Aut}\mathcal{K}(p)$ to $\mathcal{G}_h$. Therefore, we can define for any $v \geqslant 0$, the ideal $L^{(v)}_h$ in L_h as the image of $\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h) \cap (\mathrm{res}_{\mathcal{K}(p)}\mathcal{I}^{(v)}_{/\mathcal{K}})$ in $\mathcal{G}_h$. Here for any $\iota \in \mathcal{I}$, $\mathrm{res}_{\mathcal{K}(p)}\iota = \iota|_{\mathcal{K}(p)}$. Note that $\mathrm{res}_{\mathcal{K}(p)}\mathcal{I}^{(v)}_{/\mathcal{K}} = \mathcal{I}_{\mathcal{K}(p),v'}$, where $\varphi_{\mathcal{K}(p)/\mathcal{K}}(v') = v$.

Proposition 4.3. *For any $v \geqslant 0$, $\kappa_{<p}(L^{(v)}_{/\mathcal{K}}) = L^{(v)}_h$.*

We will prove it in Subsection 4.5 below.

4.4. **Ramification estimates in characteristic p.** Set for $s \in \mathbb{N}$, $\mathcal{K}[s] := \mathcal{K}^{G(\mathcal{L}(s+1))}_{<p}$ with respect to the identification $\eta_0 : \mathcal{G}_{<p} \simeq G(\mathcal{L})$. Then $\mathrm{Gal}(\mathcal{K}[s]/\mathcal{K}) = G(\mathcal{L}/\mathcal{L}(s+1))$ and $\mathcal{K}[p-1] = \mathcal{K}(p)$.

Let $v_{\mathcal{K}}[s]$ be the maximal upper ramification number of $\mathcal{K}[s]/\mathcal{K}$, i.e.

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

Proposition 4.4. *For all $s \in \mathbb{N}$, $v_{\mathcal{K}}[s] = c_0 s - 1$.*

Proof. Recall that for any $v \geqslant 0$, $\pi_f(e)(\mathcal{G}^{(v)}) = \mathcal{L}^{(v)}$ and for a sufficiently large N, the ideal $\mathcal{L}^{(v)}_k$ is generated by all $\sigma^n\mathcal{F}^0_{\gamma,-N}$, where $\gamma \geqslant v$, $n \in \mathbb{Z}$ and the elements $\mathcal{F}^0_{\gamma,-N}$ are given in [6], Subsection 1.4.

The ideal $\mathcal{L}_k^{(v)}$ is contained in the ideal generated by the monomials $\sigma^n[\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_rn_r}]$ such that $\max\{n_1, \dots, n_r\} = 0$ and $a_1p^{n_1} + \dots + a_rp^{n_r} \geqslant v$. So,

$$v \leqslant a_1 + \dots + a_r \leqslant c_0 \mathrm{wt}([\dots[D_{a_1n_1}, D_{a_2n_2}], \dots, D_{a_rn_r}]) - r\,.$$

If $v > c_0s - 1$ then $\mathrm{wt}([\dots[D_{a_1n_1}, D_{a_2n_2}], \dots D_{a_rn_r}]) > s + (r-1)/c_0$ implies that all such monomials have weight $\geqslant s+1$ and, therefore, $\mathcal{L}^{(v)} \subset \mathcal{L}(s+1)$.

If $v = c_0s - 1$ then $\mathrm{wt}([\dots[D_{a_1n_1}, D_{a_2n_2}], \dots D_{a_rn_r}]) \leqslant s$ iff $r = 1$ and the only non-zero a_i equals $c_0s - 1$. Therefore, $\mathcal{L}_k^{(v)} \operatorname{mod} \mathcal{L}_k(s+1)$ is generated by the images of all $D_{c_0s-1,n}$ and $\mathcal{L}^{(v)} \not\subset \mathcal{L}(s+1)$. ☐

Remark. This implies $v(X(K_{<p}\tilde{K})/\mathcal{K}) = v(\mathcal{K}(p)/\mathcal{K}) = c_0(p-1) - 1$. In Subsection 4.5 we prove that $v(K_{<p}/K(\pi_1)) = c_0(p-1) - 1$. This will give us the values $v[s]$ from Theorem 0.3 from Introduction.

4.5. **Proof of Proposition 4.3.** We need the following lemma.

Lemma 4.5. *Let $\eta(p) \in \mathcal{I}_{\mathcal{K}(p)}$ be the morphism from Proposition 4.1. Then $\eta(p)$ is a unique arithmetical lift of η.*

This lemma will be proved in Section 4.7 below.

Continue with the proof of Proposition 4.3.

Suppose $\tau \in \Gamma$ and for some $v \geqslant 0$, $\iota_K(\tau) \in \mathcal{I}_{/\mathcal{K}}^{(v)}$ (in particular, τ belongs to the inertia subgroup of Γ), i.e. $\mathrm{pr}_{<p}(\tau) \in L_{/\mathcal{K}}^{(v)}$.

Consider $g = \kappa(\tau) = \kappa_{<p}(\mathrm{pr}_{<p}(\tau)) \in \mathcal{G}_h$.

We can assume that $\tilde{g} \in \widetilde{\mathcal{G}}_h / C_p(\widetilde{\mathcal{G}}_h) \subset \mathrm{Aut}\mathcal{K}(p)$ is a lift of g such that for any $v' \geqslant 0$, $g \in L_h^{(v')}$ if and only if $\tilde{g} \in \mathrm{res}_{\mathcal{K}(p)} \mathcal{I}_{/\mathcal{K}}^{(v')}$. Note that in the previous notation from the definition of κ we have $\tilde{g}|_{\mathcal{K}} = \tilde{h} \in \langle h \rangle$ and $\tilde{g} = \tilde{h}(p)$.

Let $\eta := \iota_K(\tau)|_{\mathcal{K}} \tilde{h}^{-1} \in \mathcal{I}_{\mathcal{K}}$ and $\eta(p) := \iota_K(\tau)|_{\mathcal{K}(p)} \tilde{g}^{-1} \in \mathcal{I}_{\mathcal{K}(p)}$. Clearly, $\eta(p)|_{\mathcal{K}} = \eta$.

By the definition of $\tilde{h}$, $\iota_K(\tau)(t) \equiv \tilde{h}(t) \operatorname{mod} t^{(p-1)c_0+1}R$. This implies that for any $a \in \mathbb{Z}^0(p)$,

$$\eta(t^{-a}) - t^{-a} \in t^{-a+(p-1)c_0}R \tag{4.3}$$

and, therefore, $(\mathrm{id}_{\mathcal{L}} \otimes \eta)e \equiv e \operatorname{mod} t^{(p-1)c_0} \mathcal{M}_{R_0}$. From the definition of κ it follows also that $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta(p))\bar{f} = \bar{f}$, and by Lemma 4.5, $\eta(p)$ is arithmetical lift of η.

By (4.3), there is $v^o > (p-1)c_0 - 1$ such that $\eta \in \mathcal{I}_{\mathcal{K},v^o}$. Therefore, $\eta(p) \in \mathrm{res}_{\mathcal{K}(p)} \mathcal{I}_{/\mathcal{K}}^{(v^o)}$, or equivalently,

$$\iota_K(\tau)|_{\mathcal{K}(p)} \equiv \tilde{g} \operatorname{mod} \mathrm{res}_{\mathcal{K}(p)} \mathcal{I}_{/\mathcal{K}}^{(v^o)}\,.$$

So, for all $0 \leqslant v \leqslant (p-1)c_0 - 1$ and $\tau \in \Gamma_K$,

$$\mathrm{pr}_{<p}(\tau) \in L_{/\mathcal{K}}^{(v)} \quad \Leftrightarrow \quad \kappa_{<p}(\mathrm{pr}_{<p}\tau) \in L_h^{(v)}\,.$$

It remains to prove that if $v^o > (p-1)c_0 - 1$ then $L_{/\mathcal{K}}^{(v^o)} = L_h^{(v^o)} = 0$.

Suppose $\tau \in \Gamma$ is such that $\mathrm{pr}_{<p}(\tau) \in L_{/\mathcal{K}}^{(v^o)}$. We can assume that $\iota_K(\tau) \in \mathcal{I}_{/\mathcal{K}}^{(v^o)}$. Let $m \in \mathbb{Z}_p$ be such that $\iota_K(\tau)(t) = t\varepsilon^m$. Then $m \equiv 0 \bmod p$ because $\iota_K(\tau)|_{\mathcal{K}} \in \mathcal{I}_{\mathcal{K},v^o}$ and $v^o > c_0$.

Let $\hat{\tau}_0 \in \Gamma$ be such that $\hat{\tau}_0(\pi_1) = \pi_1\zeta_1$ and for any p^n-th root of unity ζ_n, $\hat{\tau}_0(\zeta_n) = \zeta_n$. Note that $\iota_K(\hat{\tau}_0)|_{\mathcal{K}} \in \mathcal{I}_{\mathcal{K},c_0}$ and $\iota_K(\hat{\tau}_0)(t) = t\varepsilon$. This implies that $\hat{\tau}_0^{-m}\tau \in \Gamma_{\widetilde{K}}$ and $\iota_K(\hat{\tau}_0^{-m}\tau) \in \mathcal{G} = \mathrm{Gal}(\mathcal{K}_{sep}/\mathcal{K})$.

Using that $\kappa(\hat{\tau}_0)^p = e$ we obtain $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \iota_K(\hat{\tau}_0^p))\bar{f} = \bar{f}$. By Lemma 4.5, $\iota_K(\hat{\tau}_0^p)|_{\mathcal{K}(p)}$ is arithmetical over $\mathcal{K}$. But $\iota_K(\hat{\tau}_0{}^p)|_{\mathcal{K}} \in \mathcal{I}_{\mathcal{K},(p-1)c_0}$ and, therefore, $\iota_K(\hat{\tau}_0^p)|_{\mathcal{K}(p)} \in \mathrm{res}_{\mathcal{K}(p)}\mathcal{I}_{/\mathcal{K}}^{((p-1)c_0)}$ and

$$\iota_K(\hat{\tau}_0^{-m}\tau)|_{\mathcal{K}(p)} \in \mathrm{res}_{\mathcal{K}(p)}\mathcal{I}_{/\mathcal{K}}^{(v')} \cap \mathrm{Gal}(\mathcal{K}(p)/\mathcal{K}) = \mathrm{Gal}(\mathcal{K}(p)/\mathcal{K})^{(v')},$$

where $v' = \min\{(p-1)c_0, v^o\} > (p-1)c_0 - 1$. By the ramification estimate from Proposition 4.4 this ramification subgroup is trivial and $\iota_K(\hat{\tau}_0^{-m}\tau)|_{\mathcal{K}(p)} = e$.

It remains to note that $\kappa_{<p}(\mathrm{pr}_{<p}\tau) = \kappa(\tau) = \kappa(\hat{\tau}_0^{-m}\tau)$ appears as the image of $\iota_K(\hat{\tau}_0^{-m}\tau)|_{\mathcal{K}(p)}$ under the natural projection of $\widetilde{\mathcal{G}}_h/C_p(\widetilde{\mathcal{G}}_h)$ to $\mathcal{G}_h$. Therefore, $\kappa_{<p}(\mathrm{pr}_{<p}\tau) = 0$ and $\mathrm{pr}_{<p}\tau = 0$.

For similar reasons, $L_h^{(v^o)} = 0$ if $v^o > (p-1)c_0 - 1$.

Proposition 4.3 is proved.

4.6. **Main results.** Theorems 0.1-0.4 are stated in the Introduction.

• *Proof of Theorem 0.1.*

By Proposition 4.3 a lift $\tau_{<p}$ is good if and only if the lift $\kappa_{<p}(\tau_{<p})$ is good. It remains to apply Theorem 2.4.

• *Proof of Theorem 0.2.*

Recall that $\Gamma_{<p}^{(v)} = G(L_{/\mathcal{K}}^{(v')})$, where $v' = \varphi_{\widetilde{K}/K}(v)$ and $e^* = c_0$.

— *If $v' > c_0$ then $L_{/\mathcal{K}}^{(v')}$ coincides with the image $\bar{\mathcal{L}}^{(v')}$ of $\mathcal{L}^{(v')}$ in $\bar{\mathcal{L}}$.*

Indeed, if $v' > (p-1)c_0 - 1$ then $L_{/\mathcal{K}}^{(v')} = 0$, cf. the proof of Proposition 4.3. By Proposition 4.4, $\bar{\mathcal{L}}^{(v')}$ is also zero.

Now suppose $c_0 < v' \leqslant (p-1)c_0 - 1$ and $\bar{\tau} \in L_{/\mathcal{K}}^{(v')}$. Let $\tau \in \Gamma^{(v)}$ be such that $\mathrm{pr}_{<p}(\tau) = \bar{\tau}$. Then (in notation from Section 4.5) there is $m \in p\mathbb{Z}_p$ such that $\hat{\tau}_0^{-m}\tau \in \Gamma_{\widetilde{K}}$ and $\iota_K(\hat{\tau}_0^{-m}\tau)|_{\mathcal{K}(p)}$ belongs to $\mathrm{res}_{\mathcal{K}(p)}(\mathcal{I}_{/\mathcal{K}}^{(v')} \cap \mathcal{G}) = \mathrm{res}_{\mathcal{K}(p)}\mathcal{G}^{(v')}$. As a result, $\kappa_{<p}(\bar{\tau}) = \kappa(\hat{\tau}_0^{-m}\tau))$ and, therefore, $\bar{\tau}$ belong to $\bar{\mathcal{L}}^{(v')}$. The opposite embedding $\bar{\mathcal{L}}^{(v')} \subset L_{/\mathcal{K}}^{(v')}$ is obvious.

This proves the case a) of our theorem, because if $c_0 < v' \leqslant pc_0$ then $v^* = v'$, and if $v' > pc_0$ then $v^* = c_0 + p(v - c_0) > (p-1)c_0 - 1$ and $\bar{\mathcal{L}}^{(v^*)}$ is also 0.

— *If $v \leqslant c_0$ then $L_{/\mathcal{K}}^{(v)}$ is generated by $\bar{\mathcal{L}}^{(v)}$ and the image of $\hat{\tau}_0$.*

Clearly, $\bar{\mathcal{L}}^{(v')}$ and the image of $\hat{\tau}_0$ belong to $L^{(v)}_{/\mathcal{K}}$. With above notation, if $\bar{\tau}\in L^{(v)}_{/\mathcal{K}}$ then for some $m\in\mathbb{Z}_p$, $\tau_0^{-m}\tau\in\Gamma_{\widetilde{K}}$, again $\iota_K(\hat{\tau}_0^{-m}\tau)\in\mathrm{res}_{\mathcal{K}(p)}\mathcal{G}^{(v)}$ and $\bar{\tau}\in\bar{\mathcal{L}}^{(v)}$.

It remains to note that $\hat{\tau}_0|_{K_{<p}}$ is a good lift of τ_0.

- *Proof of Theorem 0.3.*

It follows directly from Proposition 4.4.

- *Proof of Theorem 0.4*

It follows from results of Section 3 together with Proposition 4.3.

4.7. **Proof of Lemma 4.5.** The proof is based on the same idea as the proof of Theorem 2.4 but is considerably easier: we do not need the difficult technical result from [3]. This happens because we are still studying the lifts from $\mathcal{K}$ to $\mathcal{K}(p)$ but these lifts come from $\mathcal{I}_{\mathcal{K}}^{(v^o)}$, where $v^o>(p-1)c_0-1$, cf. below. (In Theorem 2.4 we worked with $v^o=c_0$.)

First of all, the condition

$$(\mathrm{id}_{\mathcal{L}}\otimes\eta)e\equiv e\,\mathrm{mod}\,t^{(p-1)c_0}\mathcal{M}_{R_0}\tag{4.4}$$

implies $\eta|_k=\mathrm{id}_k$ and $\eta(t^{-(p-1)c_0+1})\equiv t^{-(p-1)c_0+1}\,\mathrm{mod}\,\mathrm{m}_R$ (just follow the coefficient for $D_{(p-1)c_0-1,0}$). As a result, we obtain $\eta(t)\equiv t\,\mathrm{mod}\,t^{(p-1)c_0}\mathrm{m}_R$, i.e. there is $v^o>(p-1)c_0-1$ such that $\eta\in\mathcal{I}_{\mathcal{K},v^0}$.

Prove that $\mathcal{L}^{(v^o)}\subset\mathcal{L}(p)$.

It will be sufficient to verify that all generators $\mathcal{F}^0_{\gamma,-N}$ of $\mathcal{L}_k^{(v^o)}$ (where $\gamma\geqslant v^o$) belong to $\mathcal{L}(p)_k$. All such $\mathcal{F}^0_{\gamma,-N}$ are linear combinations of the commutators of the form $[\dots[D_{a_1n_1},],\dots,D_{a_mn_m}]$, where $m<p$, all $a_i\in\mathbb{Z}^0(p)$, all $n_i\leqslant 0$ and $a_1p^{n_1}+\dots+a_mp^{n_m}\geqslant v^o$. If $\mathrm{wt}(D_{a_in_i})=s_i$, then $(s_i-1)c_0\leqslant a_i<s_ic_0$ and

$$(p-1)c_0-1<v^o\leqslant a_1+\dots+a_m<(s_1+\dots+s_m)c_0\,.$$

This implies that $s_1+\dots+s_m\geqslant p$ (use that $a_1+\dots+a_m\in\mathbb{Z}$). So, all our commutators have weight $\geqslant p$ and, therefore, belong to $\mathcal{L}(p)_k$.

Now Corollary 1.4 implies that there is only one arithmetical lift of η to $\mathcal{K}(p)$. Therefore, it will be sufficient to prove that

- *if $\eta(p)$ is arithmetical lift of η then* $(\mathrm{id}_{\bar{\mathcal{L}}}\otimes\eta(p))\bar{f}=\bar{f}$.

As earlier in Section 2.3, let $e_{(p)}$ and $\varphi_{(p)}$ be the ramification index and, resp., the Herbrand function for $\mathcal{K}(p)/\mathcal{K}$.

Suppose

$$v^o\geqslant\varphi_{(p)}(e_{(p)}(p-1)c_0)\,.\tag{4.5}$$

Then $\eta(p)\in\mathcal{I}_{\mathcal{K}(p),v^o_{(p)}}$, where $v^o_{(p)}\geqslant e_{(p)}(p-1)c_0$ and, therefore, $(\mathrm{id}_{\bar{\mathcal{L}}}\otimes\eta(p))\bar{f}=\bar{f}$ (use that for any $a\in\mathcal{K}(p)$, $\eta(p)a-a\in at^{(p-1)c_0}R)$). This proves our lemma under assumption (4.5).

Otherwise, we can apply the trick from Section 2 as follows.

We use the notation from the beginning of Section 2.3.

Take $\mathcal{K}' = \mathcal{K}(r^o, N^o)$, where the parameters $r^o \in \mathbb{Q}$ and $N^o \equiv 0 \bmod N_0$ satisfy the following requirements (this can be done by enlarging (if necessary) N^o with fixed r^o, cf. Subsection 2.3):

$\bullet_1$) $r^o(q^o - 1) \in \mathbb{Z}^+(p)$ where $q^o = p^{N^o}$ and $(p-1)c_0 - 1 < r^o < v^o$;

$\bullet_2$) $r^o(1 - 1/q^o) > (p-1)c_0 - 1$;

$\bullet_3$) $r^o + q^o(v^o - r^o) \geqslant \varphi_{(p)}(e_{(p)}(p-1)c_0)$.

Use the uniformiser t' to define an analog $e' = \sum_{a \in \mathbb{Z}^0(p)} t'^{-a} D_{a0} \in \mathcal{L}_{\mathcal{K}'}$ of e for $\mathcal{K}'$ and set $e'^{(q^o)} = \sigma^{N^o} e' = \sum_{a \in \mathbb{Z}^0(p)} t'^{-aq^o} D_{a0} \in \mathcal{L}_{\mathcal{K}'}$.

Verify that $\bullet_2$) implies $e \equiv e'^{(q^o)} \bmod t^{(p-1)c_0} \mathcal{M}_{R_0}$. Indeed:

1) Suppose $a \geqslant (p-1)c_0$. Then $t^{-a} D_{a0}, t'^{-aq^o} D_{a0} \in \mathcal{L}(p)_{R_0}$.

2) Suppose $1 \leqslant s < p-1$ and $(s-1)c_0 \leqslant a \leqslant sc_0 - 1$, i.e. $D_{a0} \in \mathcal{L}(s)_k$. From the definition of $\mathcal{K}'$ we have $t - t'^{q^o} \in t'^{q^o + r^o(q^o - 1)} R$. This implies (use $\bullet_2$) that $t \equiv t'^{q^o} \bmod t^{(p-1)c_0} \mathrm{m}_R$ and, therefore,

$$(t^{-a} - t'^{-aq^o}) D_{a0} \in t^{-a+(p-1)c_0 - 1} \mathrm{m}_R D_{a0} \subset t^{(p-1-s)c_0} \mathcal{L}(s)_{\mathrm{m}_R} \subset t^{(p-1)c_0} \mathcal{M}_{R_0}$$

Now we can proceed similarly to the proof of Proposition 4.3 a) from [6] to obtain the existence of $m \in t^{(p-1)c_0} \mathcal{M}_{R_0}$ such that

$$e \equiv (\sigma m) \circ e'^{(q)} \circ (-m) \bmod \mathcal{L}(p)_{R_0},$$

and the existence of $f' \in \mathcal{L}_{sep}$ such that $\sigma f' = e' \circ f'$ and

$$f \equiv m \circ \sigma^{N^o}(f') \bmod \mathcal{L}(p)_{R_0}. \tag{4.6}$$

Consider the fields tower $\mathcal{K} \subset \mathcal{K}' \subset \mathcal{K}'\mathcal{K}(p) \subset \mathcal{K}'(p) \subset \mathcal{K}'_{<p}$, where $\mathcal{K}'(p)$ and $\mathcal{K}'_{<p}$ are analogs of $\mathcal{K}(p)$ and, resp, $\mathcal{K}_{<p}$ for $\mathcal{K}'$. Let $\hat{\eta}'$ be an arithmetical lift of η to $\mathcal{K}'_{<p}$. Then $\eta(p) := \hat{\eta}'|_{\mathcal{K}(p)}$, $\eta'(p) := \hat{\eta}'|_{\mathcal{K}'(p)}$ and $\eta' := \hat{\eta}'|_{\mathcal{K}'}$ are arithmetical over $\mathcal{K}$.

So, $\eta' \in \mathcal{I}_{\mathcal{K}', v'^o}$, where $v'^o = r^o + q^o(v^o - r^o) \geqslant \varphi_{(p)}(e_{(p)}(p-1)c_0)$. Therefore, we can apply assumption (4.5) and (use that $\eta'(p)$ is arithmetical over η') deduce the following congruence

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta'(p)) f' \equiv f' \bmod t'^{(p-1)c_0} \mathcal{M}'_{R_0}$$

(here $\mathcal{M}'_{R_0}$ is an analogue of $\mathcal{M}_{R_0}$ for $\mathcal{K}'$). This implies that

$$(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta'(p)) \sigma^{N^o}(f') \equiv \sigma^{N^o}(f') \bmod t^{(p-1)c_0} \mathcal{M}_{R_0}$$

(use that $\sigma^{N^o} \mathcal{M}'_{R_0} \subset \mathcal{M}_{R_0}$). It remains to note that (4.6) implies now that $(\mathrm{id}_{\bar{\mathcal{L}}} \otimes \eta(p)) \bar{f} = \bar{f}$. The lemma is proved.

References

[1] V.A.Abrashkin, *Ramification filtration of the Galois group of a local field*, Proceedings of the St. Petersburg Mathematical Society, vol. III, 35-100, 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), 18-69

[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, *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

[5] V. Abrashkin, *Groups of automorphisms of local fields of period p^M and nilpotent class $< p$*, Ann. Inst. Fourier (2017) **67**, no. 2, 605-635

[6] V. Abrashkin, *Groups of automorphisms of local fields of period p and nilpotent class $< p$, I*, Int. J. Math. (2017) **28**, no. 6: 1750043

[7] 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

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

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

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

[11] 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

[12] 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

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