RAMIFICATION FILTRATION OF THE GALOIS GROUP OF A LOCAL FIELD. II

Victor A. Abrashkin

AG "Algebraische Geometrie
und Zahlentheorie"
Jägerstraße 10-11
10117 Berlin
Germany

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
53225 Bonn
Germany

MPI / 93-77

RAMIFICATION FILTRATION OF THE GALOIS GROUP OF A LOCAL FIELD. II

ABRASHKIN VICTOR A.

Arbeitsgruppe "Algebraische Geometrie und Zahlentheorie" Jägerstraße 10-11, 10117 Berlin

0. Introduction.

Let K be a local complete discrete valuation field with a perfect residue field k of characteristic $p > 0$, K_{sep} be a fixed separable closure of K, $\Gamma = \mathrm{Gal}(K_{sep}/K)$ be the absolute Galois group of K.

The group Γ has a decreasing filtration of normal subgroups $\{\Gamma^{(v)}\}_{v\geq 0}$, where for any $v \in \mathbb{Q}$, $v \geq 0$, $\Gamma^{(v)}$ is the ramification subgroup of Γ in upper numbering, [Se, ch.2].

We have: $K_{sep}^{\Gamma^{(0)}} = K_{ur}$ is the maximal unramified extension of K, $I = \bigcup_{v>0} \Gamma^{(v)}$ is the higher ramification subgroup, which is a pro-p-group (if $\mathrm{char}\, K = p$, then I is a free pro-p-group), $K_{sep}^{I} = K_{tr}$ is the maximal tamely ramified extension of K.

Let $\mathrm{char}\, K = p$ and $\widetilde{t_0}$ be a fixed uniformizer of K. Then K can be identified with the fraction field $k((\widetilde{t_0}))$ of the power series ring $k[[\widetilde{t_0}]]$.

Let $k \simeq \bar{\mathbb{F}}_p$. Under this assumption $\Gamma = \Gamma^{(0)}$, and I is the Galois group of the maximal p-extension of K_{tr}. In this paper we give an explicit description of the image of the filtration $\{\Gamma^{(v)}\}_{v>0}$ of the group I under the natural map

$$I \longrightarrow I/C_p(I),$$

where $C_p(I)$ is the minimal closed subgroup of I containing all commutators of order $\geq p$.

This result is applied to the study of the ramification filtrations of the Galois group $\Gamma(p)$ of the maximal p-extension of K and of the Galois group $\Gamma_0(p)$ of the maximal p-extension of a field $K_0 = k_0((\widetilde{t_0}))$, where $k_0 \simeq \mathbb{F}_{q_0}$ is the finite field of $q = p^{N_0}$ elements. In these cases we obtain an explicit description of the filtrations $\{\Gamma(p)^{(v)} \bmod C_p(\Gamma(p))\}_{v>0}$ and $\{\Gamma_0(p)^{(v)} \bmod C_p(\Gamma_0(p))\}_{v>0}$.

The paper is organized as follows.

In n.1 we assume that K is an arbitrary field of characteristic $p > 0$ and give a version of Artin-Schreier theory, which permits to construct efficiently any p-extension of K having Galois group of class of nilpotency $< p$. A special case of this theory, which is ajusted to the study of p-extensions of K with Galois group of exponent p (and of class of nilpotency $< p$), was constructed in [A].

Our construction is based on

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

a) an equivalence of the category of finite Lie $\mathbb{Z}_p$-algebras $\mathcal{L}$ of class of nilpotency $< p$ and the category of finite p-groups of the same class of nilpotency, c.f. [B, ch.2, n.8, exerc.4]. This equivalence is given by the functor

$$\mathcal{L} \mapsto G(\mathcal{L}),$$

where $G(\mathcal{L}) = \mathcal{L}$ as a set and the operation on $G(\mathcal{L})$ is given via the Hausdorff series in the envelopping algebra of $\mathcal{L}$:

$$l_1, l_2 \in \mathcal{L} \mapsto l_1 \circ l_2 = \log(\exp l_1 \exp l_2);$$

b) a construction of an absolutely unramified field $\mathcal{E}(K)$ of characteristic 0 having the residue field K, where we fix a lifting σ of the absolute Frobenius endormorphism σ_0 of the field K, c.f. [B-M.nn.1.1-1.3], [F, n.A1].

The formalism of this theory permits to fix an "arithmetical meaning" of generators of the Galois group of K modulo p-th commutators and to give explicitly extensions of endormorphisms of K to field extensions of K having Galois group of class of nilpotency $< p$.

Let $K = k((\widetilde{t_0}))$ be the fraction field of the formal power series ring in a variable $\widetilde{t_0}$ with coefficients in a field $k \simeq \bar{\mathbb{F}}_p$. Then

$$K_{tr} = K(\{\widetilde{t_0}^r \mid r \in \mathbb{Q}^+(p)\}),$$

where $\mathbb{Q}^+(p) = \{r \in \mathbb{Q} \mid r > 0, (r,p) = 1\}$. In n.2 we construct a profree Lie $\mathbb{Z}_p$-algebra $\widetilde{\mathcal{L}}$ and apply the theory of n.1 to construct an identification

$$\bar{\psi} : I/C_p(I) \simeq G(\mathcal{L}),$$

where $\mathcal{L} = \widetilde{\mathcal{L}}/C_p(\widetilde{\mathcal{L}})$ and $C_p(\widetilde{\mathcal{L}})$ is the closure of the ideal in $\widetilde{\mathcal{L}}$ generated by commutators of order $\geqslant p$.

The Lie algebra $\widetilde{\mathcal{L}}$ appears as a projective limit $\varprojlim_{R,N,M} \widetilde{\mathcal{L}}_{R,N,M}$, where $R \subset \mathbb{Q}^+(p)$ is a finite subset, $N \geqslant 1, M \geqslant 0$ are integers, $\widetilde{\mathcal{L}}_{R,N,M}$ is a free Lie $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra. The extension of scalars $\widetilde{\mathcal{L}}_{R,N,M,k} = \widetilde{\mathcal{L}}_{R,N,M} \otimes W_M(k)$ of this algebra has a natural system of free generators

$$\{D_{r,n} \mid r \in R, n \in \mathbb{Z}/N\mathbb{Z}\}$$

(here $W_M(k)$ are Witt vectors of length $M+1$ with coefficients in k).

In n.3 we construct a decreasing filtration of ideals $\mathcal{L}^{(v)}$, $v \in \mathbb{Q}, v > 0$, of the Lie algebra $\mathcal{L}$. By definition,

$$\mathcal{L}^{(v)} = \varprojlim_{R,N,M} \mathcal{L}^{(v)}_{R,N,M},$$

where $\mathcal{L}^{(v)}_{R,N,M}$ are ideals of the Lie algebra $\mathcal{L}_{R,N,M} = \widetilde{\mathcal{L}}_{R,N,M}/C_p(\widetilde{\mathcal{L}}_{R,N,M})$. The ideals $\mathcal{L}^{(v)}_{R,N,M} \otimes W_M(k)$ of the Lie algebra $\mathcal{L}_{R,N,M} \otimes W_M(k)$ are given by explicit generators $\mathcal{F}_{R,N,M}(\gamma, n_1)$, where $\gamma \in \mathbb{Q}, \gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}$. The expressions of these generators consist of terms of form

$$\eta(0, m_2, ..., m_s)p^i r_1[...[D_{r_1,n_1}, D_{r_2,n_2}], ..., D_{r_s,n_s}].$$

Each of these terms corresponds to a presentation of a rational number γ in the form

$$\gamma = p^i(r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}}),$$

where $1 \leqslant s < p, r_1, ..., r_s \in R$, i and $0 = m_1 \leqslant m_2 \leqslant ... \leqslant m_s < N$ are integers. Here $m_i \bmod N = n_1 - n_i$ for $2 \leqslant i \leqslant s$, and the appearance of the coefficients $\eta(0, m_2, ..., m_s) \in \mathbb{Q}^+(p)$ is related to the existence of groups of equal elements in the sequence $m_1, m_2, ..., m_s$.

In n.3.4 we formulate the main theorem, which states that the image of the ramification filtration $\{\Gamma^{(v)}\}_{v>0}$ in $I/C_p(I)$ corresponds to the filtration $\{G(\mathcal{L}^{(v)})\}_{v>0}$ under the identification $\bar{\psi}$ of n.2.

In n.3.5 we consider a version of this theorem for the case of p-extensions of the field K. Here we have the induced identification

$$\bar{\psi}(p) : \Gamma(p)/C_p(\Gamma(p)) \simeq G(\mathcal{L}(p)),$$

where $\mathcal{L}(p) = \varprojlim_{A,N,M} \mathcal{L}_{A,N,M}$, $\mathcal{L}_{A,N,M}$ are the Lie algebras from n.2 and A is a finite subset in $\mathbb{Z}^+(p) = \mathbb{Q}^+(p) \cap \mathbb{Z}$. In this situation, for any $v > 0, v \in \mathbb{Q}$, the ideal $\mathcal{L}(p)^{(v)}$ is presented in the form $\varprojlim_N \mathcal{L}(p)_N^{(v)}$, where $\mathcal{L}(p)_N^{(v)}$ is an ideal of the Lie algebra $\mathcal{L}(p)_N = \varprojlim_{A,M} \mathcal{L}_{A,N,M}$. As a consequence of the main theorem we obtain an explicitly given system of generators of the ideals $\mathcal{L}(p)_N^{(v)} \otimes W(k)$ in the Lie algebra $\mathcal{L}(p)_N \otimes W(k)$.

The proof of the main theorem (n.3.6 and n.4) is given only modulo 3-rd commutators. This case gives sufficiently full illustration of our method. In general case (i.e. modulo p-th commutators) the proof requires more careful calculations (c.f. [A], where this was done for extensions of exponent p) and will be given in a forthcoming paper.

Let $K_0 = k_0((\widetilde{t_0}))$, where $k_0 = \mathbb{F}_{q_0}, q_0 = p^{N_0}, N_0 \geqslant 1$. If $\Gamma_0(p)$ is the Galois group of the maximal p-extension of the field K_0, then there exists a natural homomorphism

$$\gamma : \Gamma(p)/C_p(\Gamma(p)) \longrightarrow \Gamma_0(p)/C_p(\Gamma_0(p)),$$

which is compatible with ramification filtrations. In n.5 we construct an identification

$$\bar{\psi}_0 : \Gamma_0(p)/C_p(\Gamma_0(p)) \simeq G(L),$$

where $L = \widetilde{L}/C_p(\widetilde{L})$ and $\widetilde{L}$ is a free Lie pro-p-algebra over $\mathbb{Z}_p$. In this case L has a natural system of generators, which can be interpreted modulo 2-nd commutators in the terms of local class field theory. The homomorphism γ can be described via some morphism of Lie algebras $\delta : \mathcal{L}(p) \longrightarrow L$, which is constructed in nn.5.3-5.4.

In nn.5.5-5.6 we apply the explicit construction of the above morphism δ to describe the filtration $\{L^{(v)}\}_{v>0}$, which corresponds to the ramification filtration under the identification $\bar{\psi}_0$. This description does not require a passage to limit: we construct generators of ideals $L^{(v)}\otimes W(\mathbb{F}_{q_0})$ of the Lie algebra $L\otimes W(\mathbb{F}_{q_0})$.

In the following paper there will be given an application of this theory to the study of the ramification filtration of the Galois group of a local field of characteristic 0 modulo p-th commutators.

This paper was done during my stay (Febr.-Sept., 1993) in the research group of Prof. H. Koch (MPG, Arbeitsgruppe "Algebr. Geom. u. Zahlentheorie", Berlin). I express my gratitude to this organisation and especially to Prof. H. Koch and Prof. E.-W. Zink for numerous discussions.

1. Artin-Schreier theory for extensions of class of nilpotency $< p$.

1.1. *Groups and Lie algebras.*

Let $\mathcal{L}_{\mathbb{Q}}$ be a free Lie algebra over $\mathbb{Q}$ with free generators U,V and $A_{\mathbb{Q}}$ be its envelopping algebra. $A_{\mathbb{Q}}$ is a free associative algebra with generators U, V and there exists a natural embedding $\mathcal{L}_{\mathbb{Q}}\subset A_{\mathbb{Q}}$. For a natural number $n\geq 1$ denote by $C_n(\mathcal{L}_{\mathbb{Q}})$ the ideal in $\mathcal{L}_{\mathbb{Q}}$, generated by all commutators of order $\geq n$. Define a degree of any monomial in $A_{\mathbb{Q}}$ by setting $\deg U=\deg V=1$ and denote by $C_n(A_{\mathbb{Q}})$ the ideal of $A_{\mathbb{Q}}$ generated (as $\mathbb{Q}$-module) by monomials of degree $\geq n$. We set $\hat{\mathcal{L}}_{\mathbb{Q}}=\varprojlim_n \mathcal{L}_{\mathbb{Q}}/C_n(\mathcal{L}_{\mathbb{Q}})$, $\hat{A}_{\mathbb{Q}}=\varprojlim_n A_{\mathbb{Q}}/C_n(A_{\mathbb{Q}})$. For any $n\geq 1$ we have

$$C_n(A_{\mathbb{Q}})\cap\mathcal{L}_{\mathbb{Q}}=C_n(\mathcal{L}_{\mathbb{Q}}),$$

therefore, there exists a natural imbedding $\hat{\mathcal{L}}_{\mathbb{Q}}\subset\hat{A}_{\mathbb{Q}}$ induced by the above imbedding $\mathcal{L}_{\mathbb{Q}}\subset A_{\mathbb{Q}}$.

Consider the Hausdorff series

$$H(U,V)=\log(\exp U\exp V)\in\hat{A}_{\mathbb{Q}}.$$

We have the following properties.

1.1.1. $H(U,V)\in\hat{\mathcal{L}}_{\mathbb{Q}}$.

This fact is very well-known as the Campbell-Hausdorff formula. In particular, one has

$$H(U,V)=U+V+\frac{1}{2}[U,V]+\frac{1}{12}[U,[U,V]]+\frac{1}{12}[V,[V,U]]-$$

$$-\frac{1}{24}[U,[V,[U,V]]]\bmod C_5(\mathcal{L}_{\mathbb{Q}}),$$

c.f. [B, ch.2, n.6, remark 2].

1.1.2. The composition law $l_1\circ l_2=H(l_1,l_2)$, where $l_1,l_2\in\hat{\mathcal{L}}_{\mathbb{Q}}$, gives the structure of the group $G(\hat{\mathcal{L}}_{\mathbb{Q}})$ on the set $\hat{\mathcal{L}}_{\mathbb{Q}}$. With respect to this structure the zero element of $\hat{\mathcal{L}}_{\mathbb{Q}}$ is the neutral element, and $-l$ is the inverse element for any $l\in\hat{\mathcal{L}}_{\mathbb{Q}}=G(\hat{\mathcal{L}}_{\mathbb{Q}})$.

Any ideal $\mathcal{J}$ of the Lie algebra $\mathcal{L}_{\mathbf{Q}}$ can be considered as a normal subgroup $G(\mathcal{J})$ of $G(\hat{\mathcal{L}}_{\mathbf{Q}})$ and $\mathcal{J} \mapsto G(\mathcal{J})$ gives one-to-one correspondence between the set of ideals of Lie algebra $\hat{\mathcal{L}}_{\mathbf{Q}}$ and the set of normal subgroups of the group $G(\hat{\mathcal{L}}_{\mathbf{Q}})$.

1.1.3. Let $\mathcal{L}$ be a free Lie $\mathbb{Z}$-algebra with free generators U, V, then $\mathcal{L}_{\mathbf{Q}} = \mathcal{L} \otimes \mathbb{Q}$. If p is some prime number and $\mathcal{L}_{\mathbb{Z}_p} = \mathcal{L} \otimes \mathbb{Z}_p$, then in evident notation one has:

for any $l_1, l_2 \in \hat{\mathcal{L}}_{\mathbb{Z}_p}, l_1 \circ l_2 \in \hat{\mathcal{L}}_{\mathbb{Z}_p} \operatorname{mod} C_p(\hat{\mathcal{L}}_{\mathbf{Q}})$, c.f. [B, ch.2, exerc.4 of n.8].

1.1.4. Let $\mathcal{A}$ be a $\mathbb{Z}_p$-algebra and $\mathcal{L}$ be a Lie $\mathcal{A}$-algebra of class of nilpotency $< p$, i.e. $C_p(\mathcal{L}) = 0$. As a consequence of the above considerations the composition law $l_1, l_2 \mapsto l_1 \circ l_2 = H(l_1, l_2)$, where $l_1, l_2 \in \mathcal{L}$, gives the group structure on the set $\mathcal{L}$. Denote this group by $G(\mathcal{L})$. Obviously, the group $G(\mathcal{L})$ and the Lie algebra $\mathcal{L}$ have the same class of nilpotency.

If $\mathcal{A} = \mathbb{Z}_p$ then the correspondence $\mathcal{L} \mapsto G(\mathcal{L})$ gives an equivalence of the category of Lie $\mathbb{Z}_p$-algebras of a given class of nilpotency $< p$ and the category of p-groups of the same class of nilpotency, c.f. [B, ch.2, exerc.4 of n.8].

We remark that any morphism $f : \mathcal{L}_1 \longrightarrow \mathcal{L}_2$ of Lie $\mathcal{A}$-algebras $\mathcal{L}_1, \mathcal{L}_2$ (of class of nilpotency $< p$) is automatically a morphism of groups $G(\mathcal{L}_1) \longrightarrow G(\mathcal{L}_2)$. If $\widetilde{\mathcal{L}}$ is a free finitely generated Lie $\mathbb{Z}_p$-algebra, $\mathcal{L} = \widetilde{\mathcal{L}}/C_p(\widetilde{\mathcal{L}})$, then $G(\mathcal{L}) \simeq \Gamma/C_p(\Gamma)$, where Γ is finitely generated free pro-p-group and $C_p(\Gamma)$ is its normal closed subgroup generated by all commutators of order $\geq p$.

1.2. *Some facts about liftings.*

1.2.1. We follow the paper [B-M, n.1.1-1.3].

Let p be a fixed prime number and L be a field of characteristic p. For nonnegative integer M denote by $O_M(L)$ a lifting of L modulo p^{M+1}. By definition $O_M(L)$ is a flat $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra such that $O_M(L)/pO_M(L) \simeq L$. These conditions characterize $O_M(L)$ uniqielly up to an isomorphism. A construction of $O_M(L)$ can be given in the terms of p-basis of the field L as follows.

Let $\{x_i\}_{i \in I}$ be a p-basis of the field L, $W_M(L)$ be the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra of Witt vectors of length $M+1$ with coefficients in L, $[a] \in W_M(L)$ be Teichmuller representative of $a \in L$. Then $O_M(L)$ is the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-subalgebra of $W_M(L)$, generated by elements of the form

$$p^j [a]^{p^{M+1-j}} \prod_{i \in I} [x_i]^{\alpha_{ij}},$$

where $a \in A, 0 \leq j \leq M, 0 \leq \alpha_{ij} < p^{M+1-j}$ and for any fixed value of j almost all α_{ij} are equal to 0. In particular, one has $[x_i] \in O_M(L)$ for any $i \in I$.

For nonnegative integers $M_1 \geq M_2$, a lifting $O_{M_2}(L)$ can be identified with the quotient $O_{M_1}(L)/p^{M_1 - M_2} O_{M_1}(L)$. A limit of this projective system of liftings $O(L) = \varprojlim_M O_M(L)$ is the valuation ring of a complete absolutely unramified field $\mathcal{E}(L)$ of characteristic 0 with the residue field L ($\mathcal{E}(L)$ is absolutely unramified $\equiv$ p is the uniformising element of $\mathcal{E}(L)$).

Let σ_0 be the absolute Frobenius endomorphism of L, i.e. $\sigma_0(l) = l^p$ for any $l \in L$. Denote by σ some lifting of σ_0 to $O_M(L)$. This means that σ is an endomorphism of the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra $O_M(L)$ and $\sigma \bmod p = \sigma_0$. Any such lifting is a flat morphism of $\mathbb{Z}/p^{M+1}\mathbb{Z}$-modules, [B-M, 1.3].

In the terms of the above explicit construction of a lifting $O_M(L)$, the lifting σ is uniquelly defined by conditions

$$\sigma([x_i]) = y_i,$$

where $i \in I$ and y_i are arbitrary elements of $O_M(L)$ such that $y_i \equiv [x_i]^p \bmod p$.

1.2.2. From the above explicit construction of $O_M(L)$ it follows that

$$W_M(L^{(p^M)}) = \{ \sum_{0\leq j\leq M} p^j [a_j]^{p^{M-j}} \mid a_0, ..., a_M \in L\} \subset O_M(L).$$

It is easy to show that if σ is an arbitrary lifting of the Frobenius morphism, then

$$\sigma^M O_M(L) \subset W_M(L^{(p^M)}),$$

and the restriction of σ to $W_M(L^{(p^M)})$ gives the standard Frobenius endomorphism of Witt vectors.

1.2.3. Let K be a given field of characteristic p. Fix a separable closure K_{sep} and some p-basis $\{x_i\}_{i\in I}$ of the field K.

Let L be a field such that $K \subset L \subset K_{sep}$. Then $\{x_i\}_{i\in I}$ is a p-basis of L. For any integer $M \geq 0$ denote by $O_M(L)$ the lifting of L modulo p^{M+1} related to the p-basis $\{x_i\}_{i\in I}$.

Under these assumptions there is a natural action of the Galois group $\Gamma = \mathrm{Gal}(K_{sep}/K)$ on $O_M(K_{sep})$ and

$$O_M(K_{sep})^H = O_M(L),$$

where $H \subset \Gamma$ is the subgroup, such that $K_{sep}^H = L$. In particular, we use the identification

$$O_M(K_{sep})^\Gamma = O_M(K).$$

So, we have the system of liftings $O_M(L)$ which is compatible on L and on M (c.f. n.1.2.1). As earlier, set $O(L) = \varprojlim_M O_M(L)$ and denote by $\mathcal{E}(L)$ the field of fractions of the ring $O(L)$.

Following the paper [F, n.A1] fix some lifting σ of the absolute Frobenius morphism of the field K to $O(K)$. This gives a compatible system of liftings σ to all $O_M(K)$. It is easy to show that for any separable extension L of K and any integer $M \geq 0$ there exists a unique lifting $\sigma_{L,M}$ of the absolute Frobenius morphism of L to $O_M(L)$ such that $\sigma_{L,M}\mid_{O_M(K)} = \sigma$. So, σ can be extended uniquelly to all $O_M(K_{sep})$ and $O(K_{sep})$. We use the same symbol σ for these extensions. Obviously, σ commutes with the action of Γ on $O(K_{sep})$.

From flatness of σ it follows that

$$O_M(K_{sep})\mid_{\sigma=\mathrm{id}} := \{\ a \in O_M(K_{sep}) \ \mid \ \sigma a = a\ \} = W_M(\mathbb{F}_p)\ (= \mathbb{Z}/p^{M+1}\mathbb{Z}).$$

Let k be some perfect subfield of K and $M \geq 0$ be any integer. Then any $a \in k$ has Teichmuller representative $[a]$ in $O_M(K)$. This element $[a]$ can be characterized by the properties: $[a] \bmod p = a$ and $\sigma([a]) = [a]^p$. The set $\{ [a] \mid a \in k \}$ generates over $\mathbb{Z}/p^{M+1}\mathbb{Z}$ a lifting of k modulo p^{M+1} which can be identified with the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra of truncated Witt vectors $W_M(k)$.

1.3. *Main theorem.*

Let K be a field of characteristic $p > 0$.

We use assumptions of n.1.2 and all above notation.

Let $\mathcal{L}$ be a finite Lie algebra over $\mathbb{Z}_p$ having class of nilpotency $< p$. For any separable extension L of K we set

$$\mathcal{L}_L = \mathcal{L} \otimes_{W(\mathbb{F}_p)} O(L).$$

Remark that if $p^{M+1}\mathcal{L} = 0$ for some integer $M \geq 0$, then

$$\mathcal{L}_L = \mathcal{L} \otimes_{W(\mathbb{F}_p)} O_M(L).$$

Let $G(\mathcal{L}_{K_{sep}})$ be the group related to $\mathcal{L}_{K_{sep}}$ (c.f. n.1.1). It is clear that σ and Γ act on $G(\mathcal{L}_{K_{sep}})$ by functoriality.

We have the following properties:

a) $\sigma : G(\mathcal{L}_{K_{sep}}) \longrightarrow G(\mathcal{L}_{K_{sep}})$ is a homomorphism and

$$G(\mathcal{L}_{K_{sep}}) \mid_{\sigma=\mathrm{id}} = G(\mathcal{L}) \; (= G(\mathcal{L}_{\mathbb{F}_p}));$$

b) if L/K is the Galois extension then the action of $\Gamma_{L/K} = \mathrm{Gal}(L/K)$ on $\mathcal{L}_L$ commutes with σ and one has $G(\mathcal{L}_L)^{\Gamma_{L/K}} = G(\mathcal{L}_K)$.

Definition. Let $a_1, a_2 \in G(\mathcal{L}_K)$. Then $a_1 \underset{R}{\sim} a_2$ if there exists $b \in G(\mathcal{L}_K)$ such that $a_2 = (-b) \circ a_1 \circ (\sigma b)$.

Obviously, R is an equivalence relation on $G(\mathcal{L}_K)$.

Theorem. *There exists one-to-one map*

$$\pi : G(\mathcal{L}_K)/R \longrightarrow \{ \textit{ conjugacy classes of } \mathrm{Hom}(\Gamma, G(\mathcal{L})) \}.$$

Remarks.

a) It follows from the proof of this theorem (c.f. below) that π is functorial on $\mathcal{L}$ and (in an obvious sense) on a pair (K, σ).

b) Let $\mathcal{L}$ be one-dimensional Lie algebra over $\mathbb{F}_p$. By choosing some generator of the $\mathbb{F}_p$-module $\mathcal{L}$ one gets identifications: $G(\mathcal{L}) = \mathbb{Z}/p\mathbb{Z}$, $G(\mathcal{L}_K) = K$. Therefore, $G(\mathcal{L}_K)/R = K/(\sigma - \mathrm{id})K$, and our theorem gives the isomorphism

$$K/(\sigma - \mathrm{id})K \simeq \mathrm{Hom}(\Gamma, \mathbb{Z}/p\mathbb{Z})$$

of Artin-Schreier theory.

c) If $\mathcal{L}$ is a free commutative Lie algebra of rank 1 over $\mathbb{Z}/p^{M+1}\mathbb{Z}$, then we obtain Witt theory of cyclic p-extensions of K, c.f. [W], [F, n.A.2.4].

d) If $p\mathcal{L}=0$, then our theorem gives a version of Artin-Schreier theory, which was applied in [A] to the study of arbitrary extensions of K having Galois group of exponent p and class of nilpotency $< p$ (the group of p-diagonal elements in the envelopping algebra of $\mathcal{L}_K$, which we use in [A], can be identified with the group $G(\mathcal{L}_K)$ by the truncated logarithm).

Proof of theorem.

Fix an integer $M \geq 0$ such that $p^{M+1}\mathcal{L}=0$.

1.3.1. Lemma. *Let $e \in G(\mathcal{L}_K)$, then*

$$\{ f \in G(\mathcal{L}_{K_{sep}}) \mid \sigma f = f \circ e \} \neq \emptyset.$$

Proof of lemma.

We use induction on the length of $\mathbb{Z}/p^{M+1}\mathbb{Z}$-module $\mathcal{L}$. It is well-known that there exists an ideal J of the Lie algebra $\mathcal{L}$ such that $|J|=p$. Consider the exact sequence of Lie algebras

$$0 \longrightarrow J \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}' \longrightarrow 0.$$

It gives the exact sequence of p-groups

$$1 \longrightarrow G(J_{K_{sep}}) \longrightarrow G(\mathcal{L}_{K_{sep}}) \xrightarrow{\alpha} G(\mathcal{L}'_{K_{sep}}) \longrightarrow 1$$

(we use the flatness of $O_M(K_{sep})$ over $\mathbb{Z}/p^{M+1}\mathbb{Z}$).

Let

$$f' \in \{ f \in G(\mathcal{L}'_{K_{sep}}) \mid \sigma f = f \circ e' \},$$

where $e' \in G(\mathcal{L}'_K)$ is the image of e under the natural projection $G(\mathcal{L}_K) \longrightarrow G(\mathcal{L}'_K)$. If $f_1 \in G(\mathcal{L}_{K_{sep}})$ be such that $\alpha(f_1)=f'$, then

$$\sigma f_1 = f_1 \circ e + Bj,$$

where j is some generator of J and

$$B \in \mathrm{Ker}(p : O_M(K_{sep}) \longrightarrow O_M(K_{sep})) = O_0(K_{sep}) = K_{sep}$$

(we use that J is in the center of $\mathcal{L}$ and $O_M(K_{sep})$ is a flat $\mathbb{Z}/p^{M+1}\mathbb{Z}$-module).

Let $x \in K_{sep}$ be such that $x^p - x = B$ (its existence follows from Artin-Schreier theory). Set

$$f = f_1 + xj \in G(\mathcal{L}_{K_{sep}}).$$

Then

$$f \circ e = f_1 \circ e + xj,$$

$$\sigma f = \sigma f_1 + x^p j$$

and, therefore,

$$f \in \{ f \in G(\mathcal{L}_{K_{sep}}) \mid \sigma f = f \circ e \},$$

q.e.d.

1.3.2. *Construction of* π.

Construction of $\pi_f(e) \in \mathrm{Hom}(\Gamma, G(\mathcal{L}))$.

Let $e \in G(\mathcal{L}_K)$ and

$$f \in \{\ f \in G(\mathcal{L}_{K_{sep}})\ \mid\ \sigma f = f \circ e\ \}.$$

If $\tau \in \Gamma$, then $\sigma(\tau f) = \tau(\sigma f) = \tau(f \circ e) = \tau f \circ e$. Therefore,

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

$$= \tau f \circ e \circ (-e) \circ (-f) = \tau f \circ (-f).$$

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

Obviously, the correspondence $\tau \mapsto \tau f \circ (-f)$ gives the element of $\mathrm{Hom}(\Gamma, G(\mathcal{L}))$ which we denote by $\pi_f(e)$.

Dependence on f.

Let

$$f_1 \in \{\ f \in G(\mathcal{L}_{K_{sep}})\ \mid\ \sigma f = f \circ e\ \}.$$

Then

$$\sigma(f_1 \circ (-f)) = \sigma(f_1) \circ (-\sigma f) = f_1 \circ e \circ (-e) \circ (-f) = f_1 \circ (-f),$$

so, $f_1 = g \circ f$ for some $g \in G(\mathcal{L})$. By this reason, for any $\tau \in \Gamma$

$$\pi_{f_1}(e)(\tau) = g \circ \pi_f(e)(\tau) \circ (-g).$$

Therefore, $\pi_{f_1}(e)$ and $\pi_f(e)$ are in a same conjugacy class of $\mathrm{Hom}(\Gamma, G(\mathcal{L}))$ and the correspondence $e \mapsto \pi_f(e)$ gives the map

$$\tilde{\pi} : G(\mathcal{L}_K) \longrightarrow \{\text{ conj. classes of } \mathrm{Hom}(\Gamma, G(\mathcal{L}))\ \}.$$

Dependence on R.

Let $e_1, e_2 \in G(\mathcal{L}_K)$ and $e_1 \underset{R}{\sim} e_2$, i.e. $e_1 = (-b) \circ e_2 \circ (\sigma b)$ for some $b \in G(\mathcal{L}_K)$. Then for

$$f_i \in \{\ f \in G(\mathcal{L}_{K_{sep}})\ \mid\ \sigma f = f \circ e_i\ \},$$

where $i = 1, 2$, one has $(-f_1) \circ \sigma f_1 = (-b) \circ (-f_2) \circ (\sigma f_2) \circ (\sigma b)$, i.e.

$$f_2 \circ b \circ (-f_1) = g \in G(\mathcal{L}_{K_{sep}})\mid_{\sigma=\mathrm{id}} = G(\mathcal{L}).$$

So, for any $\tau \in \Gamma$,

$$\pi_{f_2}(e_2)(\tau) = \tau f_2 \circ (-f_2) = g \circ (\tau f_1) \circ (-b) \circ b \circ (-f_1) \circ (-g) =$$

$$= g \circ \pi_{f_1}(e_1)(\tau) \circ (-g)$$

and $\tilde{\pi}$ defines the map

$$\pi : G(\mathcal{L}_K)/R \longrightarrow \{ \text{ conj. classes of } \operatorname{Hom}(\Gamma, G(\mathcal{L})) \ \}.$$

1.3.3. *Injectivity of* π.

Let $e_1, e_2 \in G(\mathcal{L}_K)$ be such that $\tilde{\pi}(e_1) = \tilde{\pi}(e_2)$. If, for $i = 1, 2$,

$$f_i \in \{ \ f \in G(\mathcal{L}_{K_{sep}}) \ \mid \ \sigma f = f \circ e_i \ \},$$

then for some $g \in G(\mathcal{L})$ and any $\tau \in \Gamma$

$$\pi_{f_1}(e_1)(\tau) = g \circ \pi_{f_2}(e_2)(\tau) \circ (-g).$$

This means that $\tau f_1 \circ (-f_1) = g \circ \tau f_2 \circ (-f_2) \circ (-g)$, i.e.

$$(-f_2) \circ (-g) \circ f_1 = h \in G(\mathcal{L}_{K_{sep}})^{\Gamma} = G(\mathcal{L}_K).$$

Therefore, $f_1 = g \circ f_2 \circ h, \sigma f_1 = g \circ \sigma f_2 \circ \sigma h$ and

$$e_1 = (-f_1) \circ (\sigma f_1) = (-h) \circ (-f_2) \circ (-g) \circ g \circ f_2 \circ e_2 \circ \sigma h = (-h) \circ e_2 \circ \sigma h.$$

So, $e_1 \underset{R}{\sim} e_2$ and π is injective.

1.3.4. *Surjectivity of* π.

We proceed by induction on the length of $\mathcal{L}$ and use notation of n.1.3.1. Let

$$\eta \in \operatorname{Hom}(\Gamma, G(\mathcal{L}))$$

and

$$\eta' \in \operatorname{Hom}(\Gamma, G(\mathcal{L}'))$$

be its image under the projection

$$\operatorname{Hom}(\Gamma, G(\mathcal{L})) \longrightarrow \operatorname{Hom}(\Gamma, G(\mathcal{L}')).$$

Then there exist $e' \in G(\mathcal{L}'_K)$ and

$$f' \in \{ \ f \in G(\mathcal{L}'_{K_{sep}}) \ \mid \sigma f = f \circ e' \ \}$$

such that $\eta'(\tau) = (\tau f') \circ (-f')$.

Let $e \in G(\mathcal{L}_K)$ be some preimage of the e' under the projection $G(\mathcal{L}_K) \longrightarrow G(\mathcal{L}'_K)$. It follows from the proof of Lemma 1.3.1 that the natural map of sets

$$\{ \ f \in G(\mathcal{L}_{K_{sep}}) \ \mid \ \sigma f = f \circ e \ \} \longrightarrow \{ \ f \in G(\mathcal{L}'_{K_{sep}}) \ \mid \ \sigma f = f \circ e' \ \}$$

is surjective. Therefore, there exists $f \in G(\mathcal{L}_{K_{sep}})$ such that $\sigma f = f \circ e$ and $\pi_f(e)(\tau) \equiv \eta(\tau) \operatorname{mod} G(J)$ for any $\tau \in \Gamma$.

Therefore,

$$\eta(\tau) = \pi_f(e)(\tau) + c_\tau j,$$

for some $c_\tau \in \mathbb{F}_p$ (as in n.1.3.1 we use that J is in the center of $\mathcal{L}$ and $O_M(\mathbb{F}_p)$ is a flat module).

Obviously, $\tau \mapsto c_\tau$ defines the element of $\mathrm{Hom}(\Gamma, \mathbb{F}_p)$. From Artin-Schreier theory it follows the existence of $x \in K_{sep}$ such that $c_\tau = \tau x - x$ for any $\tau \in \Gamma$.

Let $f^* = f + xj \in G(\mathcal{L}_{K_{sep}})$. Then $\eta(\tau) = (\tau f^*) \circ (-f^*)$. On the other hand

$$(-f^*) \circ (\sigma f^*) = (x^p - x)j \circ (-f) \circ (\sigma f) = e + (x^p - x)j.$$

For any $\tau \in \Gamma$,

$$\tau(x^p - x) = (x + c_\tau)^p - (x + c_\tau) = x^p - x,$$

therefore, for $e^* = e + (x^p - x)j \in G(\mathcal{L}_K)$, we have

$$f^* \in \{ \, f \in G(\mathcal{L}_{K_{sep}}) \mid \sigma f = f \circ e^* \, \}$$

and $\eta = \pi_{f^*}(e^*)$.

Theorem is proved.

1.4. Corollary. *Let (in notation of n.1.3) $\eta \in \mathrm{Hom}(\Gamma, G(\mathcal{L}))$. Then there exist $e \in G(\mathcal{L}_K)$ and*

$$f \in \{ \, G(\mathcal{L}_{K_{sep}}) \mid \sigma f = f \circ e \, \}$$

such that $\eta = \pi_f(e)$.

1.5. In notation of n.1.3 let $e \in G(\mathcal{L}_K)$ be such that the conjugacy class $\pi(e)$ (c.f. theorem of n.1.3) contains an epimorphism $\eta : \Gamma \longrightarrow G(\mathcal{L})$ (and, therefore, all elements of $\pi(e)$ are epimorphic maps $\Gamma \longrightarrow G(\mathcal{L})$). Set $K_e = K_{sep}^{\mathrm{Ker}\,\eta}$, then η defines the isomorphism of the groups $\mathrm{Gal}(K_e/K)$ and $G(\mathcal{L})$.

Let b be an automorphism of the field K, $\hat{b}$ be an extension of b to some automorphism of K_{sep}.

Let $M \geqslant 0$ be an integer, such that $p^{M+1}\mathcal{L} = 0$. Generally, there is no lifting of b to an automorphism of $O_M(K)$, which commutes with σ (but, if such lifting exists then it is defined uniquelly). Nevertheless, there exists a lifting of $b|_{K^{(p^M)}}$ to a morphism

$$\sigma^M O_M(K) \longrightarrow O_M(K).$$

This morphism commutes with σ and is induced by the embeddings (c.f. n.1.1.2)

$$\sigma^M O_M(K) \subset W_M(K^{(p^M)}) \subset O_M(K)$$

and the morphism

$$W_M(b|_{K^{(p^M)}}) : W_M(K^{(p^M)}) \longrightarrow W_M(K^{(p^M)}).$$

We shall use the same symbol b for this lifting. Analogously, we use the same notation $\hat{b}$ for the lifting of the above chosen extension $\hat{b}$ of the automorphism b.

If a is an automorphism of the Lie algebra $\mathcal{L}$, then we use the same symbol a for extension of scalars $\mathcal{L}_L \longrightarrow \mathcal{L}_L$ of the morphism a (L is some field of characteristic p). Clearly, actions of a and σ on $\mathcal{L}_L$ commute one with another.

1.5.1. Proposition. *In the above notation the following statements are equivalent:*

1. $\hat{b}(K_e) = K_e$*;*

2. There exists an automorphism a of the Lie algebra $\mathcal{L}$*, such that* $b(\sigma^M e) \underset{R}{\sim} a(e)$.

Proof.

Let $\hat{b}(K_e) = K_e$.

Choose $f \in G(\mathcal{L}_{K_{sep}})$ such that $\sigma f = f \circ e$ and $\eta = \pi_f(e)$ (c.f. n.1.4). Then for any $\tau \in \Gamma_K$ we have $\eta(\tau) = \tau f \circ (-f)$.

Let $f_1 = \hat{b}(\sigma^M f)$. Then $\sigma(f_1) = f_1 \circ b(\sigma^M e)$. For any $\tau \in \Gamma_K$ we have

$$\pi_{f_1}(b(\sigma^M e))(\tau) = \tau f_1 \circ (-f_1) = \hat{b}[(\hat{b}^{-1}\tau\hat{b})\sigma^M f \circ (-\sigma^M f)] =$$

$$= \hat{b}[(\hat{b}^{-1}\tau\hat{b})f \circ (-f)] = \eta(\hat{b}^{-1}\tau\hat{b}).$$

The equality $\hat{b}(K_e) = K_e$ gives $\hat{b}^{-1}(\operatorname{Ker}\eta)\hat{b} = \operatorname{Ker}\eta$, therefore, there exists an automorphism a of the group $G(\mathcal{L})$ (which is also an automorphism of the Lie algebra $\mathcal{L}$), such that $\pi_{f_1}(b(\sigma^M e)) = \eta a$.

For any $\tau \in \Gamma_K$

$$\tau(f_1) \circ (-f_1) = \pi_{f_1}(b(\sigma^M e))(\tau) = a(\eta(\tau)) = a(\tau f \circ (-f)) = \tau(af) \circ (-af).$$

Therefore,

$$(-af) \circ f_1 = c \in G(\mathcal{L}_{K_{sep}})^{\Gamma} = G(\mathcal{L}_K).$$

Applying the morphism σ to the equality $f_1 = (af) \circ c$ one obtains

$$\sigma f_1 = f_1 \circ (b(\sigma^M e)) = (af) \circ c \circ (b(\sigma^M e)),$$

$$\sigma f_1 = \sigma(af) \circ \sigma c = (af) \circ (ae) \circ \sigma c.$$

Therefore, $b(\sigma^M e) = (-c) \circ a(e) \circ \sigma(c)$, i.e. $b(\sigma^M e) \underset{R}{\sim} a(e)$.

Inversely, let

$$b(\sigma^M e) = (-c) \circ a(e) \circ \sigma(c)$$

for some $c \in G(\mathcal{L}_K)$. From the equality $\sigma f_1 = f_1 \circ b(\sigma^M e)$ one has

$$\sigma(f_1 \circ (-c)) = f_1 \circ (-c) \circ a(e).$$

Now the equality $\sigma(af) = a(f) \circ a(e)$ gives the existence of $c_0 \in G(\mathcal{L})$, such that

$$f_1 \circ (-c) = c_0 \circ a(f).$$

This means that

$$\pi_{f_1}(b(\sigma^M e)) = \tau(f_1) \circ (-f_1) = c_0 \circ [\tau(af) \circ (-af)] \circ (-c_0).$$

Now it is clear that

$$\tau \in \operatorname{Ker}\eta \Leftrightarrow \tau f = f \Leftrightarrow \tau(af) = af \Leftrightarrow \tau \in \operatorname{Ker}\pi_{f_1}(b(\sigma^M e)).$$

Proposition is proved.

1.5.2. *Remark.*

Let b can be extended to some automorphism of the algebra $O_M(K)$, which commutes with σ. Denote this extension by the same symbol b. Then

$$b(\sigma^M e) = \sigma^M(be) \underset{R}{\sim} b(e).$$

In addition, let a be an automorphism of the Lie algebra $\mathcal{L}$ and $c \in G(\mathcal{L}_K)$ be such that $b(e) = (-c) \circ a(e) \circ \sigma(c)$. Then the correspondence $f \mapsto a(f) \circ c$ gives an explicit description of liftings of b to automorphisms of the field K_e.

1.5.3. Corollary. *Let (in the above notation) K be the Galois extension of its subfield K_1. Then the following properties are equivalent:*

1. K_e/K_1 is the Galois extension.

2. For any $b \in \mathrm{Gal}(K/K_1)$ there exists an automorphism a_b of the Lie algebra $\mathcal{L}$ such that $b(\sigma^M e) \underset{R}{\sim} a_b(e)$.

1.5.4. *Remark.*

Let $b \in \mathrm{Gal}(K/K_1)$. Consider a morphism a_b from the above corollary as an automorphism of the group $G(\mathcal{L})$. Then there exists a lifting $\hat{b} \in \mathrm{Gal}(K_{sep}/K_1)$ of b and an epimorphism $\eta \in \pi(e)$, such that for any $\tau \in \Gamma_K$ one has

$$\pi(\hat{b}^{-1}\tau\hat{b}) = a_b(\eta(\tau)).$$

This means that a_b gives a description of the action of the quotient $\mathrm{Gal}(K/K_1)$ on the subgroup $\mathrm{Gal}(K_e/K)$ by conjugation with respect to the identification $\mathrm{Gal}(K_e/K) = G(\mathcal{L})$, given by the epimorphism η.

2. Case of a local field.

2.1. Let K be a local complete discrete valuation field of characteristic $p > 0$ with a residue field k which is isomorphic to an algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. Then K is isomorphic to $k((\tilde{t}_0))$ - the fraction field of the power series ring in one variable $\tilde{t}_0$ over k.

Let K_{sep} be a fixed separable closure of K and $\Gamma = \mathrm{Gal}(K_{sep}/K)$. If

$$\mathbb{Q}^+(p) = \{\ r \in \mathbb{Q} \ \mid\ r > 0, (r,p) = 1\ \}$$

and $K_{tr} \subset K_{sep}$ is the maximal tamely ramified extension of K, then

$$K_{tr} = K(\{\ \tilde{t}_0^{\,r} \ \mid\ r \in \mathbb{Q}^+(p)\ \}).$$

Here $\{\ \tilde{t}_0^{\,r} \mid r \in \mathbb{Q}^+(p)\ \}$ is a compatible system of fraction powers of $\tilde{t}_0$ (this means that for any $r \in \mathbb{Q}^+(p), m \in \mathbb{Z}^+(p) = \mathbb{Q}^+(p) \cap \mathbb{Z}$, one has the equality $(\tilde{t}_0^{\,r})^m = \tilde{t}_0^{\,mr}$).

Let I be the higher ramification subgroup of Γ. Then I is a free pro-p-group. We want to apply the arguments of n.1 to the study of the extension $K_{sep}^{C_p(I)}$ of K.

Fix absolutely unramified field $\mathcal{E}(K_{sep})$ (c.f. n.1.2) and consider its valuation ring $O(K_{sep})$. Let H be an open subgroup of Γ, $L = K_{sep}^H$ and M be some nonnegative integer, then

$$O_M(L) = O(K_{sep})^H / p^{M+1} O(K_{sep})^H$$

is a lifting of L modulo p^{M+1}.

Let $\tilde{t}$ be some fixed lifting of the uniformising element $\tilde{t_0} \in K$ to $O(K_{sep})$. Then $O_M(K)$ can be identified with the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra of Laurent series in one variable $\tilde{t}$ with coefficients in $W_M(k)$.

We can fix some lifting σ of the absolute Frobenius morphism of the field K by choosing some $\sigma\tilde{t} \in O(K_{sep})$, which satisfies the condition

$$\sigma\tilde{t} \equiv \tilde{t}^p \bmod p$$

(in fact, we use below the simplest choice of such a lifting, which is given by the equality $\sigma\tilde{t} = \tilde{t}^p$).

2.2. Let $M \geq 0, N \geq 1$ be integers, R be a finite subset of $\mathbb{Q}^+(p)$. Set $q = p^N$ and introduce a free $\mathbb{Z}/p^{M+1}\mathbb{Z}$-module $L^\circ_{R,M}$ with fixed (free) generators D°_r, $r \in R$.

Denote by $\tilde{\mathcal{L}}_{R,N,M}$ the free Lie $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra with the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-module of free generators

$$L^\circ_{R,M} \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p))$$

(here $W_M(\mathbb{F}_q)$ and $W_M(\mathbb{F}_p)(\simeq \mathbb{Z}/p^{M+1}\mathbb{Z})$ are the groups of truncated Witt vectors having length $M+1$ and coefficients from $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively).

Let $\tilde{\mathcal{L}}_{R_1,N_1,M_1}$ and $\tilde{\mathcal{L}}_{R_2,N_2,M_2}$ be such Lie algebras, where $R_2 \subset R_1$, $N_2|N_1$ and $M_2 \leq M_1$. We have the natural map of their modules of free generators:

$$L^\circ_{R_1,M_1} \otimes \mathrm{Hom}(W_{M_1}(\mathbb{F}_{p^{N_1}}), W_{M_1}(\mathbb{F}_p)) \longrightarrow L^\circ_{R_2,M_2} \otimes \mathrm{Hom}(W_{M_2}(\mathbb{F}_{p^{N_2}}), W_{M_2}(\mathbb{F}_p)).$$

This map is uniquelly defined by the following conditions:

$$D^\circ_r \mapsto D^\circ_r, \text{ if } r \in R_2,$$

$$D^\circ_r \mapsto 0, \text{ if } r \in R_1 \setminus R_2,$$

$$f \mapsto f\,|_{W_{M_2}(\mathbb{F}_{p^{N_2}})},$$

where $f \in \mathrm{Hom}(W_{M_1}(\mathbb{F}_{p^{N_1}}), W_{M_1}(\mathbb{F}_p))$ and $W_{M_2}(\mathbb{F}_{p^{N_2}})$ is considered as a subgroup of $W_{M_1}(\mathbb{F}_{p^{N_1}})$ via the natural imbeddings:

$$W_{M_2}(\mathbb{F}_{p^{N_2}}) \subset W_{M_2}(\mathbb{F}_{p^{N_1}}) = p^{M_1-M_2} W_{M_1}(\mathbb{F}_{p^{N_1}}) \subset W_{M_1}(\mathbb{F}_{p^{N_1}}).$$

The above maps give uniquelly defined morphisms of the Lie algebras $\tilde{\mathcal{L}}_{R_1,N_1,M_1} \longrightarrow \tilde{\mathcal{L}}_{R_2,N_2,M_2}$. So, we have a projective system of Lie algebras $\{\tilde{\mathcal{L}}_{R,N,M}\}$. Obviously,

$$\tilde{\mathcal{L}} = \varprojlim_{R,N,M} \tilde{\mathcal{L}}_{R,N,M}$$

is the free Lie pro-p-algebra over $\mathbb{Z}_p$.

2.3. Let

$$\mathcal{L}_{R,N,M} = \widetilde{\mathcal{L}}_{R,N,M}/C_p(\widetilde{\mathcal{L}}_{R,N,M}).$$

We obtain a projective system $\{\mathcal{L}_{R,N,M}\}$ of Lie algebras of class of nilpotency $< p$. If $\mathcal{L} = \varprojlim_{R,N,M} \mathcal{L}_{R,N,M}$, then $\mathcal{L} = \widetilde{\mathcal{L}}/C_p(\widetilde{\mathcal{L}})$ (here $C_p(\widetilde{\mathcal{L}})$ is the closure of the ideal in $\widetilde{\mathcal{L}}$ generated by all commutators of order $\geq p$).

We want to apply main theorem of n.1 to the projective system $\{\mathcal{L}_{R,N,M}\}$.

If $r \in R$ and $f \in \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p))$, we use notation $D_{r,f}$ for the image of

$$D_r^\circ \otimes f \in L_{R,M}^\circ \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p)) \subset \widetilde{\mathcal{L}}_{R,N,M}$$

in $\mathcal{L}_{R,N,M}$.

Let $\{\alpha_i\}_{1 \leqslant i \leqslant N}$ be some $W_M(\mathbb{F}_p)$-basis of $W_M(\mathbb{F}_q)$ and $\{f_i\}_{1 \leq i \leq N}$ be dual basis of the $W_M(\mathbb{F}_p)$-module $\mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p))$. Consider

$$e_{R,N,M} = \sum_{\substack{1 \leqslant i \leqslant N \\ r \in R}} \alpha_i t^r D_{r,f_i} \in G(\mathcal{L}_{R,N,M,K_{tr}})$$

(we use all notation of n.1), where $t = \widetilde{t}^{\,-1}$ (c.f. n.2.1). This element $e_{R,N,M}$ does not depend on the above choice of a basis in $W_M(\mathbb{F}_q)$, because

$$e_{R,N,M} = (\sum_{r \in R} t^r D_r^\circ) \otimes (\sum_{1 \leq i \leq N} \alpha_i \otimes f_i)$$

and $\sum_{1 \leq i \leq N} \alpha_i \otimes f_i$ corresponds to $\mathrm{id}_{W_M(\mathbb{F}_q)}$ under the identification

$$W_M(\mathbb{F}_q) \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p)) = \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_q)).$$

So, we have the element $\{e_{R,N,M}\}$ of the projective system $\{G(\mathcal{L}_{R,N,M,K_{tr}})\}$, which gives

$$e = \varprojlim_{R,N,M} e_{R,N,M} \in G(\mathcal{L}_{K_{tr}}) = \varprojlim_{R,N,M} G(\mathcal{L}_{R,N,M,K_{tr}}).$$

2.4. Let

$$\mathcal{M}_{R,N,M} = \{\ f \in G(\mathcal{L}_{R,N,M,K_{sep}}) \ \mid\ \sigma f = f \circ e_{R,N,M}\ \}.$$

Obviously, $\{\mathcal{M}_{R,N,M}\}$ is a projective system of sets and

$$\mathcal{M} = \varprojlim_{R,N,M} \mathcal{M}_{R,N,M} \neq \emptyset.$$

Let $f \in \mathcal{M}$ and $f_{R,N,M}$ be its projection to $\mathcal{M}_{R,N,M}$. Consider the homomorphism

$$\psi_{R,N,M} = \pi_{f_{R,N,M}}(e_{R,N,M}) : I \longrightarrow G(\mathcal{L}_{R,N,M})$$

from the proof of the main theorem of n.1 (here $I = \mathrm{Gal}(K_{sep}/K_{tr})$). In the same way as in [A,n.2.3], we obtain:

a) all $\psi_{R,N,M}$ are epimorphisms;

b) the system $\{\psi_{R,N,M}\}$ is a projective system, compatible (in an obvious sense) with the projective system $\{G(\mathcal{L}_{R,N,M})\}$;

c) the homomorphism

$$\psi = \varprojlim_{R,N,M} \psi_{R,N,M} : I \longrightarrow G(\mathcal{L})$$

induces the isomorphism

$$\bar{\psi} : I/C_p(I) \simeq G(\mathcal{L}).$$

We use $\bar{\psi}$ below for identification of the groups $I/C_p(I)$ and $G(\mathcal{L})$.

2.5. One can apply remarks of n.1.5 for a description of the action of the Galois group $\mathrm{Gal}(K_{tr}/\mathbb{F}_p((\tilde{t}_0))$ on $I/C_p(I)$ in the terms of the identification $\bar{\psi}$. For simplicity we assume that the lifting σ is given by the condition $\sigma\tilde{t} = \tilde{t}^p$.

The group Γ_{tr} has two generators ϕ_0 and τ_0, which satisfy the unique relation $\tau_0^p = \phi_0^{-1}\tau_0\phi_0$. One has

a) ϕ_0 is the lifting of the absolute Frobenius morphism of the extension $k/\mathbb{F}_p$, uniquelly determined by the condition $\phi_0(\tilde{t}_0) = \tilde{t}_0$.

b) τ_0 is some generator of the procyclic group $I_{tr} = \mathrm{Gal}(K_{tr}/K) \subset \Gamma_{tr}$, τ_0 acts trivially on k, $\tau_0\tilde{t}_0^{\,r} = \zeta_r\tilde{t}_0^{\,r}$, where $r \in \mathbb{Q}^+(p), \zeta_r \in k$.

The system of elements $\{\zeta_r \mid r \in \mathbb{Q}^+(p)\}$ satisfies the following two conditions:

1) $\zeta_1 = 1$;

2) for any $r_1 \in \mathbb{Q}^+(p), m \in \mathbb{Z}^+(p) = \mathbb{Q}^+(p) \cap \mathbb{Z}$, one has $\zeta_r^m = \zeta_{mr}$.

It is easy to see that a fixing of such a system of elements $\zeta_r, r \in \mathbb{Q}^+(p)$, is equivalent to the choice of some generator τ_0 of the group I_{tr}.

The automorphisms ϕ_0 and τ_0 can be lifted to automorphisms ϕ and τ of the algebra $O(K_{tr})$, which are defined by the following conditions:

$$\phi|_{W(k)} = W(\phi_0), \quad \phi(\tilde{t}) = \tilde{t};$$

$$\tau|_{W(k)} = \mathrm{id}, \quad \tau(\tilde{t}^{\,r}) = [\zeta_r]\tilde{t}^{\,r}.$$

Obviously, ϕ and τ commute with the action of σ on $O(K_{tr})$.

Consider the element $e = \varprojlim_{R,N,M} e_{R,N,M}$ from n.2.3. From the relations

$$\phi(e_{R,N,M}) = \sum_{\substack{r\in R\\ 1\leq i\leq N}} \sigma(\alpha_i)t^r D_{r,f_i}, \qquad \tau(e_{R,N,M}) = \sum_{\substack{r\in R\\ 1\leq i\leq N}} \alpha_i[\zeta_r]^{-1}t^r D_{r,f_i}$$

one gets

a) $\phi(e) = a_\phi(e)$, where a_ϕ is the automorphism of the Lie algebra $\mathcal{L}$ such that

$$a_\phi(D_{r,f}) = D_{r,\phi^*(f)},$$

where $D_{r,f} \in \mathcal{L}_{R,N,M}$ and $\phi^*(f)(w) = f(\phi w)$ for any $w \in W(\mathbb{F}_{p^N})$;

b)$\tau(e) = a_\tau(e)$, where a_τ is the automorphism of the Lie algebra $\mathcal{L}$, such that

$$a_\tau(D_{r,f}) = D_{r,\tau_r(f)},$$

where $D_{r,f} \in \mathcal{L}_{R,N,M}, r(p^N-1) \in \mathbb{N}$ and $\tau_r(f)(w) = f([\zeta_r]w)$ for any $w \in W(\mathbb{F}_{p^N})$.

Therefore (c.f. remark 1.5.2), we can fix liftings $\hat{\phi}, \hat{\tau} \in \mathrm{Gal}(K_{sep}/\mathbb{F}_p((\widetilde{t_0})))/C_p(I)$ of the automorphisms ϕ_0 and τ_0 by the following conditions:

$$\hat{\phi}(f) = a_\phi(f), \quad \hat{\tau}(f) = a_\tau(f).$$

Applying remark 1.5.4 one gets for any $g \in I/C_p(I)$:

$$\bar{\psi}(\hat{\phi}^{-1} g \hat{\phi}) = a_\phi(\bar{\psi}(g)), \quad \bar{\psi}(\hat{\tau}^{-1} g \hat{\tau}) = a_\tau(\bar{\psi}(g)).$$

3. Statement of the main theorem.

In this section we define a decreasing filtration $\{\mathcal{L}^{(v)}\}_{v>0}$ of ideals $\mathcal{L}^{(v)}$ of the Lie algebra $\mathcal{L}$ from n.2.3, where $v \in \mathbb{Q}$, $v > 0$. This filtration will be related to the image of the ramification filtration $\{\Gamma^{(v)}\}_{v>0}$ of Γ in $I/C_p(I)$.

3.1. Let $\widetilde{\mathcal{L}}_{R,N,M}$ be some Lie algebra from the projective system $\{\widetilde{\mathcal{L}}_{R,N,M}\}$ (c.f. n.2.3). Then $\widetilde{\mathcal{L}}_{R,N,M} \otimes_{W_M(\mathbb{F}_p)} W_M(k)$ has the $W_M(k)$-module of free generators

$$\begin{aligned} &L^\circ_{R,M} \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_p)) \otimes W_M(k) = \\ &= L^\circ_{R,M} \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_q)) \otimes_{W_M(\mathbb{F}_q)} W_M(k) = \\ &= L^\circ_{R,M} \otimes \mathrm{Hom}_{W_M(\mathbb{F}_q)}(W_M(\mathbb{F}_q) \otimes W_M(\mathbb{F}_q), W_M(\mathbb{F}_q)) \otimes_{W_M(\mathbb{F}_q)} W_M(k) = \\ &= \bigoplus_{n \in \mathbb{Z}/N\mathbb{Z}} L^\circ_{R,M} \otimes \mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_q))_n \otimes_{W_M(\mathbb{F}_p)} W_M(k), \end{aligned}$$

where $\mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_q))_n, n \in \mathbb{Z}/N\mathbb{Z}$, is the $W_M(\mathbb{F}_p)$-module of σ^n-linear homomorphisms $W_M(\mathbb{F}_q) \longrightarrow W_M(\mathbb{F}_q)$. Obviously, each module

$$\mathrm{Hom}(W_M(\mathbb{F}_q), W_M(\mathbb{F}_q))_n$$

has $W_M(\mathbb{F}_p)$-rank 1 and the canonical generator σ^n.

Therefore, the Lie $W_M(k)$-algebra $\widetilde{\mathcal{L}}_{R,N,M,k} = \widetilde{\mathcal{L}}_{R,M,N} \otimes_{W_M(\mathbb{F}_p)} W_M(k)$ has the canonical system of free generators

$$\{ D^\circ_r \otimes \sigma^n \mid r \in R, n \in \mathbb{Z}/N\mathbb{Z} \}.$$

Denote by $D_{r,n}$, where $r \in R, n \in \mathbb{Z}/N\mathbb{Z}$, the image of $D^\circ_r \otimes \sigma^n$ under the canonical projection

$$\widetilde{\mathcal{L}}_{R,M,N,k} \longrightarrow \mathcal{L}_{R,M,N,k}.$$

Remark.

Let a_ϕ and a_τ be the automorphisms of the Lie algebra $\mathcal{L}$, which were introduced earlier to describe the action of the Galois group $\mathrm{Gal}(K_{tr}/\mathbb{F}_p((\widetilde{t_0})))$ (c.f. n. 2.5) on $I/C_p(I)$. Extension of scalars of these automorphisms defines automorphisms of the Lie algebra $\mathcal{L}_k$, which we denote by the same symbols. In the terms of generators $\{D_{r,n} \mid r \in R, n \in \mathbb{Z}/N\mathbb{Z}\}$ the action of a_ϕ and a_τ is given on $\mathcal{L}_{R,N,M,k}$ by the following conditions:

a) $a_\phi(D_{r,n}) = D_{r,n+1}$;

b) $a_\tau(D_{r,n}) = [\zeta_r]^{p^n} D_{r,n}$,

where $r \in R, r(p^N-1) \in \mathbb{N}$ and $n \in \mathbb{Z}/N\mathbb{Z}$.

3.2. Let $1 \le s < p$.

Definition. If $m_1, ..., m_s \geqslant 0$ are integers, we set

$$\eta(m_1, ..., m_s) = \frac{1}{s_1!(s_2 - s_1)!...(s_l - s_{l-1})!},$$

if $m_1 = ... = m_{s_1} < m_{s_1+1} = ... = m_{s_2} < ... < m_{s_{l-1}} = ... = m_{s_l}$, where $1 \leq s_1 < ... < s_l = s$, and

$$\eta(m_1, ..., m_s) = 0,$$

otherwise.

Let $N \in \mathbb{N}$ and $n_1, ..., n_s \in \mathbb{Z}/N\mathbb{Z}$.

Definition. For indices $1 \leq i, j \leq s$, n_{ij} will denote the integer uniquelly defined by the following conditions: $n_{ij} \bmod N = n_i - n_j, 0 \leq n_{ij} < N$.

Definition. $\tilde{\eta}(n_1, ..., n_s) = \eta(n_{11}, n_{12}, ..., n_{1s})$.

Remark. $\tilde{\eta}(n_1, ..., n_s) \neq 0 \Leftrightarrow$ the sequence of points $\{e^{\frac{2\pi i n_j}{N}}\}_{1 \leq j \leq s}$ is "ordered" on a unit circle $\{z \in \mathbb{C} \mid |z| = 1\}$.

3.3. Let $\mathcal{L}_{R,N,M}$ be some Lie algebra from the projective system $\{\mathcal{L}_{R,N,M}\}$ (c.f. the beginning of n.2.3). For any $\gamma \in \mathbb{Q}, \gamma > 0$, and $n_1 \in \mathbb{Z}/N\mathbb{Z}$ introduce elements $\mathcal{F}_{R,N,M}(\gamma, n_1) \in \mathcal{L}_{R,N,M,k}$ $(= \mathcal{L}_{R,N,M} \otimes W_M(k))$:

$$\mathcal{F}_{R,N,M}(\gamma, n_1) =$$

$$= \sum_{1 \leq s < p} (-1)^s \sum_{\substack{r_1, ..., r_s \in R \\ n_2, ..., n_s \in \mathbf{Z}/N\mathbf{Z} \\ i \in \mathbf{Z}, i \geqslant 0 \\ p^i \left(r_1 + \frac{r_2}{p^{n_{12}}} + ... + \frac{r_s}{p^{n_{1s}}}\right) = \gamma}} p^i r_1 \tilde{\eta}(n_1, ..., n_s)[...[D_{r_1, n_1+i}, D_{r_2, n_2+i}], ..., D_{r_s, n_s+i}].$$

Definition. Let $v \in \mathbb{Q}, v > 0$. Denote by $\mathcal{L}^{(v)}_{R,N,M,k}$ the ideal of the Lie $W_M(k)$-algebra $\mathcal{L}_{R,N,M,k}$, which is generated by all $\mathcal{F}_{R,N,M}(\gamma, n)$, where $\gamma \geqslant v$ and $n \in \mathbb{Z}/N\mathbb{Z}$.

Let

$$\mathcal{L}_{R_1,N_1,M_1} \longrightarrow \mathcal{L}_{R_2,N_2,M_2},$$

where $R_2 \subset R_1, N_2 | N_1, M_2 \leq M_1$, be the connecting morphism of the projective system of Lie algebras $\{\mathcal{L}_{R,N,M}\}$. If $N_1 = N_2$, then this morphism, obviously, induces the epimorphic mapping of ideals

$$\mathcal{L}^{(v)}_{R_1,N_1,M_1} \longrightarrow \mathcal{L}^{(v)}_{R_2,N_2,M_2},$$

for any $v > 0, v \in \mathbb{Q}$. This property, generally, is not valid for $N_1 \neq N_2$. Nevertheless, we have the following proposition.

3.3.1. Proposition. *For any $v \in \mathbb{Q}, v > 0$, and a finite subset $R \subset \mathbb{Q}^+(p)$, there exists a natural number $\widetilde{N} = \widetilde{N}(R, v)$ such that the system*

$$\{\mathcal{L}^{(v)}_{R,N,M} \mid N \geq \widetilde{N}(R,v)\ \}_{R,N,M}$$

is a projective system of Lie algebras, whose connecting morphisms are epimorphisms, induced by connecting morphisms of the projective system $\{\mathcal{L}_{R,N,M}\}_{R,N,M}$.

Proof.

The proof of this statement is a slight modification of the proof of Proposition 4.4 of [A].

Let $\gamma \in \mathbb{Q}, \gamma > 0$.

We call a presentation of γ in the form

$$\gamma = p^i(r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}})$$

R-admissible, if $1 \leqslant s < p$, $r_1, ..., r_s \in R$, $i, m_1 = 0, m_2, ..., m_s$ are nonnegative integers, and $m_2 \leq ... \leq m_s$. It is easy to see that the set of different R-admissible presentations of the given rational number γ is finite.

As in [A, loc.cit.], one can prove the existence of a finite set $\mathcal{M}(R, v)$ of rational numbers $\gamma \geqslant v$, having the following property:

if $\gamma_1 \in \mathbb{Q}, \gamma_1 \geqslant v$ and

$$\gamma_1 = p^i(r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}})$$

is R-admissible presentation of γ_1, then there exist $\gamma = \gamma(\gamma_1) \in \mathcal{M}(R, v)$ and an index $s_1 = s_1(\gamma_1) \leq s$ such that

a)

$$\gamma = p^i(r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_{s_1}}{p^{m_{s_1}}});$$

b) if $\gamma = p^{i^*}(r_1^* + \frac{r_2^*}{p^{m_2^*}} + ... + \frac{r_l^*}{p^{m_l^*}})$ is any R-admissible prersentation of γ, then $m_l^* < m_{s_1+1}$.

Let $\widetilde{N}(R, v)$ be a natural number, satisfying the following implication:

if $\gamma \in \mathcal{M}(R, v)$ and

$$\gamma = p^i(r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}})$$

is some R-admissible presentation of γ, then $m_s < \widetilde{N}(R, v)$.

It is clear, that such $\widetilde{N}(R, v)$ exists.

Now following [A, loc.cit.] one can show that if $N \geqslant \widetilde{N}(R, v)$, then

1) the ideal $\mathcal{L}^{(v)}_{R,N,M,k}$ is generated by the finite set of elements $\mathcal{F}_{R,N,M}(\gamma, n_1)$, where $\gamma \in \mathcal{M}(R, v)$ and $n_1 \in \mathbb{Z}/N\mathbb{Z}$;

2) if $N_1, N_2 \geqslant \widetilde{N}(R, v), N_2 | N_1, M_2 \leq M_1, \gamma \in \mathcal{M}(R, v), n \in \mathbb{Z}/N_1\mathbb{Z}$, then

$$\mathcal{F}_{R,N_1,M_1}(\gamma, n) \mapsto \mathcal{F}_{R,N_2,M_2}(\gamma, n \bmod N_2)$$

under the connecting morphism $\mathcal{L}_{R,N_1,M_1} \longrightarrow \mathcal{L}_{R,N_2,M_2}$ and, therefore, $\mathcal{L}^{(v)}_{R,N_1,M_1,k}$ is mapped onto $\mathcal{L}^{(v)}_{R,N_2,M_2,k}$.

Proposition is proved.

Remark. Let $1 \leq s < p$. One can consider the projective system

$$\{\mathcal{L}_{R,N,M} \bmod C_{s+1}(\mathcal{L}_{R,N,M})\}_{R,N,M}$$

and the analogous statement for the system of ideals

$$\{\mathcal{L}^{(v)}_{R,N,M} \bmod C_{s+1}(\mathcal{L}_{R,N,M})\}_{R,N,M}.$$

As in the above Proposition it is sufficient to find a natural number $\widetilde{N}_s(R,v)$ such that, for any $N_1, N_2 \geq \widetilde{N}_s(R,v), N_2|N_1$ and $M_2 \leq M_1$ the epimorphic map $\mathcal{L}_{R,N_1,M_1} \longrightarrow \mathcal{L}_{R,N_2,M_2}$ induces the epimorphism

$$\mathcal{L}^{(v)}_{R,N_1,M_1,k} \bmod C_{s+1}(\mathcal{L}_{R,N_1,M_1,k}) \longrightarrow \mathcal{L}^{(v)}_{R,N_2,M_2,k} \bmod C_{s+1}(\mathcal{L}_{R,N_2,M_2,k}).$$

It is clear that $\widetilde{N}_s(R,v) = \widetilde{N}(R,v)$ satisfies this implication, but for a given value of s this choice can be done more economically.

One can verify, for example, that $\widetilde{N}_1(R,v) = 1$ and

$$\widetilde{N}_2(R,v) = \max\{n \in \mathbb{N} \mid \exists r_1, r_2 \in R, i \in \mathbb{Z}, i \geq 0 \text{ such that } p^i(r_1 + \frac{r_2}{p^{n-1}}) \geq v, p^i r_1 < v, p^i r_2 < v\}.$$

3.3.2. Using the above Proposition, for any $v \in \mathbb{Q}, v > 0$, one can define the ideals

$$\mathcal{L}^{(v)}_k = \varprojlim_{R,N,M} \mathcal{L}^{(v)}_{R,N,M,k}$$

of the Lie algebra $\mathcal{L}_k = \mathcal{L} \otimes_{O(\mathbb{F}_p)} O(k)$.

Let $\mathcal{L}^{(v)} = \mathcal{L}^{(v)}_k |_{\sigma=\mathrm{id}}$, where the action of σ on $\mathcal{L}^{(v)}_k$ is given by its standard action as the Frobenius automorphism on $O(k) \simeq W(k)$ and by the equalities $\sigma D_{r,n} = D_{r,n+1}$, where $r \in R, n \in \mathbb{Z}/N\mathbb{Z}$, and $D_{r,n}$ are the topological generators of $\mathcal{L}^{(v)}_k$, introduced in n.3.1.

Obviously, all $\mathcal{L}^{(v)}$ are ideals of the Lie $\mathbb{Z}_p$-algebra $\mathcal{L}$, $\mathcal{L}^{(v)}O(k) = \mathcal{L}^{(v)}_k$ in $\mathcal{L}_k$ and $\{\mathcal{L}^{(v)}\}_{v>0}$ is a decreasing filtration of $\mathcal{L}$.

Remark.

Let $v > 0, v \in \mathbb{Q}$ and $\mathcal{L}^{[v]}_{R,N,M}$ be the image of the ideal $\mathcal{L}^{(v)}$ under the canonical map

$$\mathcal{L} = \varprojlim_{R,N,M} \mathcal{L}_{R,N,M} \longrightarrow \mathcal{L}_{R,N,M}.$$

It follows now that the ideal $\mathcal{L}^{[v]}_{R,N,M,k}$ is generated by

$$\mathcal{F}^*_{R,N,M}(\gamma, n_1) = \sigma^{n_1}\mathcal{F}^*_{R,N,M}(\gamma, 0),$$

where $\gamma \in \mathbb{Q}, \gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}$ and

$$\mathcal{F}^*_{R,N,M}(\gamma, 0) =$$

$$= \sum_{\substack{1 \leq s < p \\ r_1, \ldots, r_s \in R \\ i, m_2, \ldots, m_s \geqslant 0 \\ p^i \left(r_1 + \frac{r_2}{p^{m_2}} + \ldots + \frac{r_s}{p^{m_s}}\right) = \gamma}} (-1)^s p^i r_1 \eta(0, m_2, \ldots, m_s)[\ldots[D_{r_1, j_N(i)}, D_{r_2, j_N(i-m_2)}], \ldots, D_{r_s, j_N(i-m_s)}].$$

Here η is function defined in the beginning of n.3.2 and for any integer m $j_N(m)$ is the notation for the residue of m modulo N.

3.4. We use notation and assumptions of n.2.1. In addition we assume, that *the lifting σ is given by the condition $\sigma\tilde{t} = \tilde{t}^p$.*

Let $\{\Gamma^{(v)}\}_{v \geq 0}$ be the ramification filtration of the Galois group $\Gamma = \mathrm{Gal}(K_{sep}/K)$ of our local field K in upper numbering, c.f. [Se, 2[e] part.]. This filtration is a decreasing filtration of normal subgroups $\Gamma^{(v)}, v \in \mathbb{Q}, v > 0$, and the higher ramification subgroup I equals to $\bigcup_{v>0} \Gamma^{(v)}$.

Let $\mathcal{L}$ be the Lie pro-p-algebra from n.2.3 and $\psi : I \longrightarrow G(\mathcal{L})$ be the homomorphism of groups which we use in n.2.4 for the identification

$$\bar{\psi} : I/C_p(I) \simeq G(\mathcal{L}).$$

Let $\{\mathcal{L}^{(v)}\}_{v>0}$ be the decreasing filtration of ideals of the Lie algebra $\mathcal{L}$ introduced in n.3.3. Then $\{G(\mathcal{L}^{(v)})\}_{v>0}$ is a decreasing filtration of the group $G(\mathcal{L})$ by its normal subgroups $G(\mathcal{L}^{(v)})$.

Theorem. *For any $v > 0, v \in \mathbb{Q}$,*

$$\psi(\Gamma^{(v)}) = G(\mathcal{L}^{(v)}),$$

i.e. the image of the ramification filtration $\{\Gamma^{(v)}\}_{v>0}$ in $I/C_p(I)$ and the filtration $\{G(\mathcal{L}^{(v)})\}_{v>0}$ coincide under the identification $\bar{\psi}$.

Remarks.

a) The definition of ramification subgroups $\Gamma^{(v)}$ and ideals $\mathcal{L}^{(v)}$ can be given for any real $v \in \mathbb{R}$, $v \geq 0$. Also, the proof of the above Theorem is valid for all real positive values of v. But this does not give more general result, because of the left-continuty of these two filtrations. Indeed, for any $v_0 \in \mathbb{R}, v_0 > 0$, the equality

$$\Gamma^{(v_0)} = \bigcap_{0<v<v_0} \Gamma^{(v)}$$

is a formal consequence of the equalities

$$\Gamma^{(v_0)}_{L/K} = \bigcap_{0<v<v_0} \Gamma^{(v)}_{L/K}$$

for all finite Galois extensions L/K, which are valid by definition, [Se, loc.cit.]. The filtration $\{\mathcal{L}^{(v)}\}_{v>0}$ is left-continuos by the same reason.

b) Let $\mathcal{L}_0 = \mathcal{L} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$, then the identification $\bar{\psi}$ induces the identification

$$\bar{\psi}_0 : I/I^pC_p(I) \simeq G(\mathcal{L}_0).$$

If ψ_0 is the composition of $\bar{\psi}_0$ with the natural projection $I \longrightarrow I/I^pC_p(I)$ and $\{\mathcal{L}_0^{(v)}\}_{v>0}$ is the image of the filtration $\{\mathcal{L}^{(v)}\}_{v>0}$ under the natural projection $\mathcal{L} \longrightarrow \mathcal{L}_0$, then our Theorem gives for any $v \in \mathbb{Q}, v > 0$, the following equality

$$\psi_0(\Gamma^{(v)}) = G(\mathcal{L}_0^{(v)}).$$

So, we obtain a description of the ramification filtration of the maximal p-extension of K_{tr} with Galois group of exponent p and class of nilpotency $< p$. This statement was proved in [A] where we use more general choice of identification of the groups $I/I^pC_p(I)$ and $G(\mathcal{L}_0)$.

3.5. *Case of p-extensions of the field K.*

Before proving the above Theorem we give some of its corollaries related to the ramification filtration of the Galois group of the maximal p-extension of K.

3.5.1. Let $\{\mathcal{L}_{A,N,M}\}$ be the subsystem of the projective system of Lie algebras $\{\mathcal{L}_{R,N,M}\}$ from n.2.3. Here $A \subset \mathbb{Z}^+(p) = \mathbb{Q}^+(p) \cap \mathbb{Z}$ is arbitrary finite set, $N \geqslant 1, M \geqslant 0$ are integers.

Let $\mathcal{L}(p) = \varprojlim_{A,N,M} \mathcal{L}_{A,N,M}$ and

$$\pi(p) : \mathcal{L} \longrightarrow \mathcal{L}(p)$$

be the natural projection. It is clear that

$$\pi(p) = \varprojlim_{R,N,M} \pi(p)_{R,N,M},$$

where the morphisms

$$\pi(p)_{R,N,M,k} = \pi(p)_{R,N,M} \otimes W_M(k) : \mathcal{L}_{R,N,M,k} \longrightarrow \mathcal{L}_{A(R),N,M,k}$$

are given by the following conditions

$$D_{r,n} \mapsto 0, \text{ if } r \in R \setminus \mathbb{Z}^+(p);$$

$$D_{r,n} \mapsto D_{r,n}, \text{ if } r \in A(R) = R \cap \mathbb{Z}^+(p).$$

3.5.2. Let $\Gamma(p)$ be the Galois group of the maximal p-extension of K, $j(p) : I \longrightarrow \Gamma(p)$ be the natural projection. Then there exists a unique homomorphism $\psi(p) : \Gamma(p) \longrightarrow G(\mathcal{L}(p))$ such that

a) $\pi(p) \cdot \psi = \psi(p) \cdot j(p)$

(here ψ is the homomorphism from n.2.4);

b) $\psi(p)$ belongs to the equivalence class related by Theorem of n.1.3 to the element

$$e(p) = \varprojlim_{A,N,M} \sum_{a \in A} t^a D_{a,0} \in G(\mathcal{L}(p)_K);$$

c) if $f(p) = \pi(p)_{K_{sep}}(f)$, where $f \in G(\mathcal{L}_{K_{sep}})$ is the element from n.2.4, then for any $\tau \in \Gamma(p)$ one has:

$$\psi(p)(\tau) = \tau f(p) \circ (-f(p)).$$

d) $\bar{\psi}(p) = \psi(p) \bmod C_p(\Gamma(p))$ defines the identification of the groups $\Gamma(p)/C_p(\Gamma(p))$ and $G(\mathcal{L}(p))$.

3.5.3. Let $\mathcal{L}(p) = \varprojlim_N \mathcal{L}(p)_N$, where $\mathcal{L}(p)_N = \varprojlim_{A,M} \mathcal{L}_{A,N,M}$. Remark that $\mathcal{L}(p)_{N,k} = \mathcal{L}(p)_N \otimes W(k)$ is a pro-p-algebra with the set of topological generators

$$\{D_{a,n} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N\mathbb{Z}\}.$$

For any $v \in \mathbb{Q}, v > 0$, denote by $\{\mathcal{L}(p)^{(v)}\}_{v>0}$ the filtration related to the image of the filtration $\{\Gamma(p)^{(v)}\}_{v>0}$ in the group $\Gamma(p)/C_p(\Gamma(p))$ via the identification $\bar{\psi}(p)$.

Let $\{\mathcal{L}(p)_N^{(v)}\}_{v>0}$ and $\{\mathcal{L}(p)_{A,N,M}^{(v)}\}_{v>0}$ be the images of the filtration $\{\mathcal{L}(p)^{(v)}\}_{v>0}$ under the canonical projections $\mathcal{L}(p) \longrightarrow \mathcal{L}(p)_N$ and $\mathcal{L}(p) \longrightarrow \mathcal{L}_{A,N,M}$.

For any $v \in \mathbb{Q}, v > 0$, the set of elements

$$\{\mathcal{F}^*_{A,N,M}(\gamma, n_1) \mid \gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}\}$$

generates the ideal $\mathcal{L}(p)_{A,N,M,k}^{(v)} = \mathcal{L}(p)_{A,N,M}^{(v)} \otimes W(k)$ in the Lie algebra $\mathcal{L}_{A,N,M,k}$ (c.f. n.3.3.2).

Using the explicit expressions for the elements $\mathcal{F}^*_{A,N,M}(\gamma, n_1)$, one can obtain the following lemma:

Lemma. *If $1 \leqslant s_0 < p, a \in A \subset \mathbb{Z}^+(p), m \in \mathbb{Z}/N\mathbb{Z}$, $p^i a \geqslant s_0 v$, then*

$$p^i D_{a,m} \in \mathcal{L}(p)_{A,N,M,k}^{(v)} \bmod C_{s_0+1}(\mathcal{L}(p)_{A,N,M,k}).$$

3.5.4. As earlier, for any $l \in \mathbb{Z}$ $j_N(l)$ is the residue of l modulo N.

Proposition. *For any $v \in \mathbb{Q}, v > 0$, the ideal $\mathcal{L}(p)_{N,k}^{(v)} = \mathcal{L}(p)_N^{(v)} \otimes W(k)$ is generated by the following elements:*

a) $p^i D_{a,n}$, where $a \in \mathbb{Z}^+(p), i \geqslant 0$ is an integer, $n \in \mathbb{Z}/N\mathbb{Z}$ and $p^i a \geqslant (p-1)v$;

b) $\mathcal{F}_{N,v}(\gamma, n_1) = \sigma^{n_1} \mathcal{F}_{N,v}(\gamma, 0)$, where $\gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}$ and

$$\mathcal{F}_{N,v}(\gamma, 0) =$$

$$= \sum_{\substack{1 \leqslant s < p \\ a_1, \ldots, a_s \in \mathbb{Z}^+(p) \\ i, m_2, \ldots, m_s \geqslant 0 \\ p^i\left(a_1 + \frac{a_2}{p^{m_2}} + \ldots + \frac{a_s}{p^{m_s}}\right) = \gamma \\ p^i a_1, \ldots, p^i a_s < (p-s)v}} (-1)^s p^i a_1 \eta(0, m_2, \ldots, m_s)[\ldots[D_{a_1, j_N(i)}, D_{a_2, j_N(i-m_2)}], \ldots, D_{a_s, j_N(i-m_s)}].$$

Proof.

From Lemma of n.3.5.3 it follows that the ideal $\mathcal{L}(p)^{(v)}_{A,N,M,k}$ is generated by the following elements:

a) $p^iD_{a,n}$, where $a \in A$ and $p^ia \geqslant (p-1)v$;

b) $\mathcal{F}^{**}_{A,N,M}(\gamma, n_1) = \sigma^{n_1}\mathcal{F}^{**}_{A,N,M}(\gamma, 0)$, where $\gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}$, and the expression for $\mathcal{F}^{**}_{A,N,M}(\gamma, 0)$ is obtained from the expression of $\mathcal{F}^{*}_{A,N,M}(\gamma, 0)$ by introducing the restrictions $p^ia_1, ..., p^ia_s < (p-s)v$.

In order to finish the proof one need only remark that for sufficiently large set $A \subset \mathbb{Z}^+(p)$ and a natural number M (e.g. $A \supset [1, (p-1)v\ ) \cap \mathbb{Z}^+(p)$ and $p^M \geqslant \gamma$) the sequence

$$\{\mathcal{F}^{**}_{A,N,M}(\gamma, n_1)\}_{A,M}$$

is stationary and its limit is equal to $\mathcal{F}_{N,v}(\gamma, n_1)$.

3.5.5. Analogously, one can obtain the following proposition:

Proposition. *Let $1 \leqslant s_0 < p, v \in \mathbb{Q}, v > 0$. Then the ideal*

$$\mathcal{L}(p)^{(v)}_{N,k} \bmod C_{s_0+1}(\mathcal{L}(p)_{N,k})$$

is generated by the following elements:

a) $p^iD_{a,n}$, where $i \geqslant 0, a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N\mathbb{Z}$ and $p^ia \geqslant s_0v$;

b) $\mathcal{F}_{N,v,s_0}(\gamma, n_1) = \sigma^{n_1}\mathcal{F}_{N,v,s_0}(\gamma, 0)$, where $\gamma \geqslant v, n_1 \in \mathbb{Z}/N\mathbb{Z}$ and

$$\mathcal{F}_{N,v,s_0}(\gamma, 0) =$$

$$= \sum_{\substack{1\leqslant s\leqslant s_0 \\ a_1,\dots,a_s\in\mathbb{Z}^+(p) \\ i,m_2,\dots,m_s\geqslant 0 \\ p^i\left(a_1+\frac{a_2}{p^{m_2}}+\dots+\frac{a_s}{p^{m_s}}\right)=\gamma \\ p^ia_1,\dots,p^ia_s<(s_0+1-s)v}} (-1)^s p^i a_1 \eta(0, m_2, ..., m_s)[...[D_{a_1,j_N(i)}, D_{a_2,j_N(i-m_2)}], ..., D_{a_s,j_N(i-m_s)}].$$

3.6. *Restatement of the main theorem.*

For any finite extension L/K define its "largest upper ramification number" $v(L/K)$ by the following condition:

$$\Gamma^{(v)} \textit{ acts trivially on } L/K \Leftrightarrow v > v(L/K).$$

Existence of $v(L/K)$ follows from the left-continuty of the image $\{\Gamma^{(v)}_{L/K}\}_{v>0}$ of the filtration $\{\Gamma^{(v)}\}_{v>0}$ in $\Gamma_{L/K}$ (c.f. Remark a) of n.3.4).

Let $\mathcal{L} = \varprojlim_{R,N,M} \mathcal{L}_{R,N,M}$ as in n.2.3 and

$$\psi_{R,N,M} : I \longrightarrow G(\mathcal{L}_{R,N,M})$$

be the homomorphism from n.2.4. If

$$K_{R,N,M} = K_{sep}^{\operatorname{Ker}\psi_{R,N,M}},$$

then $K_{R,N,M}$ is (in an obvious sense) the field of definition of the element $f_{R,N,M} \in G(\mathcal{L}_{R,N,M,K_{sep}})$ which was chosen in n.2.4.

If $\mathcal{J}$ is any ideal of $\mathcal{L}_{R,N,M}$, then the image $f_{R,N,M} \bmod \mathcal{J}$ of $f_{R,N,M}$ under the natural projection

$$G(\mathcal{L}_{R,N,M,K_{sep}}) \longrightarrow G((\mathcal{L}_{R,N,M}/\mathcal{J})_{K_{sep}})$$

defines by functorial property of the statement of Theorem n.1.3 a homomorphism

$$I \longrightarrow G(\mathcal{L}_{R,N,M}/\mathcal{J}).$$

This homomorphism is equal to the composition of $\psi_{R,N,M}$ and the natural projection

$$G(\mathcal{L}_{R,N,M}) \longrightarrow G(\mathcal{L}_{R,N,M}/\mathcal{J}).$$

Obviously, the field of definition of $f_{R,N,M} \bmod \mathcal{J}$ equals to $K^{G(\mathcal{J})}_{R,N,M}$.

For $v_0 \in \mathbb{Q}, v_0 > 0$, denote by $\mathcal{L}_{R,N,M}(v_0)$ the ideal of $\mathcal{L}_{R,N,M}$ such that

$$\psi_{R,N,M}(\Gamma^{(v_0)}) = G(\mathcal{L}_{R,N,M}(v_0)) \subset G(\mathcal{L}_{R,N,M}).$$

Then the above arguments give the following minimal property:

(P) *$\mathcal{L}_{R,N,M}(v_0)$ is the minimal element in the family of ideals $\mathcal{J}$ of $\mathcal{L}_{R,N,M}$ such that the field of definition of $f_{R,N,M} \bmod \mathcal{J}$ has the largest upper ramification number $< v_0$.*

Let $\mathcal{L}^{(v_0)}_{R,N,M} = \mathcal{L}^{(v_0)}_{R,N,M,k}|_{\sigma=\mathrm{id}}$, where the ideals $\mathcal{L}^{(v_0)}_{R,N,M,k}$ were defined in n.3.2. Now Theorem of n.3.4 can be restated as follows:

3.6.1. Proposition. *Let $R \subset \mathbb{Q}^+(p)$ be a finite subset, $M \in \mathbb{Z}, M \geqslant 0, v_0 \in \mathbb{Q}, v_0 > 0$. Then there exists a natural number $N_0(R,M,v_0)$ such that for any $N \geqslant N_0(R,M,v_0)$ the ideal $\mathcal{L}^{(v_0)}_{R,N,M}$ of $\mathcal{L}_{R,N,M}$ satisfies the above property* **(P)**.

Let $1 \leq s < p$ and $C_{s+1}(\mathcal{L}_{R,N,M})$ be (as usually) the ideal of $\mathcal{L}_{R,N,M}$ generated by commutators of order $\geq s+1$. One can consider the minimal property (P_s) taking in the minimal property **(P)** ideals $\mathcal{J}$, which satisfy the additional requirement $\mathcal{J} \supset C_{s+1}(\mathcal{L}_{R,N,M})$.

Obviously, the above proposition is equivalent to the following one:

3.6.2. Proposition. *For $1 \leq s < p$ and R, M, v_0 as above, there exists a natural number $N_s(R,M,v_0)$ such that for any $N \geq N_s(R,M,v_0)$ the ideal*

$$\mathcal{L}^{(v_0)}_{R,N,M} + C_{s+1}(\mathcal{L}_{R,N,M})$$

satisfies the property (P_s).

Remarks.

a) In fact the proof of our Theorem modulo I^p in [A] (c.f. remark b) of n.3.4) was obtained as the proof of statements analogous to Proposition 3.6.2 by induction on s.

b) One can be not worry about a minimal possible value of $N_s(R,M,v_0)$. If proposition is proved for some choice of this constant then it will be automatically valid for all $N \geq \widetilde{N}_s(R,v_0)$, where $\widetilde{N}_s(R,v_0)$ is the natural number from remark to proposition 3.3.1.

Example.

The above statements give:

a) If $s = 1$, then $\mathcal{L}_{R,N,M,k}(v_0) \bmod C_2(\mathcal{L}_{R,N,M,k})$ is generated by elements of the set

$$\{\ p^i D_{r,n}\ \mid\ r \in R, n \in \mathbb{Z}/N\mathbb{Z}, i \in \mathbb{Z}, i \geq 0, p^i r \geq v_0\ \}.$$

b) If $s = 2$, then $\mathcal{L}_{R,N,M,k}(v_0) \bmod C_3(\mathcal{L}_{R,N,M,k})$ is generated (as ideal) for $N \geq N_2(R, M, v_0)$ by the elements $\mathcal{F}_{R,N,M}(\gamma, n_1)$ where $\gamma \in \mathbb{Q}, \gamma > 0, n_1 \in \mathbb{Z}/N\mathbb{Z}$ and

$$\mathcal{F}_{R,N,M}(\gamma, n_1) = \varepsilon(\gamma) D_{r(\gamma), n_1 + l(\gamma)} - \sum_{\substack{r_1, r_2 \in R \\ n_2 \in \mathbb{Z}/N\mathbb{Z}, i \geqslant 0 \\ p^i \left(r_1 + \frac{r_2}{p^{n_{12}}}\right) = \gamma}} p^i r_1 \tilde{\eta}(n_1, n_2) \left[D_{r_1, n_1 + i}, D_{r_2, n_2 + i}\right].$$

Here, $\varepsilon(\gamma) = 0$, if γ is not p-entier, and $\varepsilon(\gamma) = \gamma$, otherwise;

$r(\gamma) \in \mathbb{Q}^+(p)$ and $l(\gamma) \in \mathbb{Z}$ are uniquelly defined from the equality $\gamma = p^{l(\gamma)} r(\gamma)$;

$\tilde{\eta}(n_1, n_2) = 1$ if $n_1 \neq n_2$, and $\tilde{\eta}(n_1, n_2) = 1/2$ otherwise;

$n_{12} \in \mathbb{Z}$ is uniquelly defined by the conditions: $0 \leq n_{12} < N$ and $n_{12} \bmod N = n_1 - n_2$.

4. Proof of the main theorem modulo $C_3(\mathcal{L})$.

In this section we prove Theorem of n.3 modulo $C_3(\mathcal{L})$, i.e. we give the proof of proposition 3.6.2 for $s \leq 2$. We use all notation and assumptions of nn.3.4 and 3.6.

4.1. *Case* $s = 1$.

Lemma. *Let* $X \in O_M(K_{sep})$ *be such that*

$$\sigma X - X = w t^r$$

where $w \in W_M(k)$ *and* $K(X)$ *is the field of definition of* X. *Then*

$$v(K(X)/K) = \max\{\ r p^l\ \mid\ l \in \mathbb{Z}, l \geq 0, p^l w \neq 0\ \}.$$

Proof.

We can assume, that $w \in W_M(\mathbb{F}_{q_1})$ for some $q_1 = p^{N_1}$. Consider the embedding

$$j : O_M(K_{sep}) \longrightarrow W_M(K_{sep}),$$

which transforms σ to the standard Frobenius morphism of Witt vectors (c.f. for example [F, n.A1.3.2]). Therefore, j transforms $\widetilde{t}$ to Teichmuller representative of $\widetilde{t} \bmod p = \widetilde{t}_0$ (because $\sigma\widetilde{t} = \widetilde{t}^{\,p}$). Now one can use Shafarevich's basis of the group K^*, [Sh], and Witt explicit reciprocity law, [W], to get the conclusion of our lemma.

Proposition. *Let $\mathcal{L}^{(0)}$ be a commutative Lie $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra,*

$$e_0 = \sum_{r\in R} t^r A_r \in G(\mathcal{L}^{(0)}_{K_{tr}}),$$

where $A_r \in \mathcal{L}^{(0)}_k, f_0 \in G(\mathcal{L}^{(0)}_{K_{sep}})$ is such that $\pi_{f_0}(e_0) \in \pi(e_0)$ (c.f. notation of n.1) and $K(f_0) = K_{sep}^{\mathrm{Ker}\,\pi_{f_0}(e_0)}$ is the field of definition of f_0. Then the following statements are equivalent:

a) $v(K(f_0)/K) < v_0$;

b) if $r \in R, s \in \mathbb{Z}, s \geq 0$ and $p^s r \geq v_0$, then $p^s A_r = 0$.

Proof.

Let $\{B_i\}_{i\in I}$ be a special system of generators of $\mathbb{Z}/p^{M+1}\mathbb{Z}$-module $\mathcal{L}^{(0)}$, which satisfies the following condition:

$$\text{if } \sum_{i\in I} a_i B_i = 0 \text{ for } a_i \in \mathbb{Z}/p^{M+1}\mathbb{Z}, i \in I \text{ then } a_i B_i = 0 \text{ for } \forall i \in I.$$

Let $A_r = \sum_{i\in I} a_{ir} B_i$ and $f_0 = \sum_{i\in I} X_i B_i$, where all $a_{ir} \in W_M(k)$ and all $X_i \in O_M(K_{sep})$. Then

$$\sigma X_i - X_i = \sum_{r\in R} a_{ir} t^r.$$

Let K_i be the field of definition of $X_i, i \in I$. We have:

$$v(K(f_0)/K) < v_0 \Leftrightarrow v(K_i/K) < v_0 \text{ for all } i \in I,$$

because K is the composite of all $K_i, i \in I$.

It follows from the above Lemma that

$$v(K_i/K) = \max\{\, rp^l \mid r \in R, p^l a_{ir} \neq 0 \,\}.$$

So, $v(K_i/K) < v_0$ for all $i \in I$, if and only if the following implication is true:

if $r \in R$ and $rp^l \geq v_0$, then $p^l a_{ir} = 0$ for all $i \in I$.

But the condition "$p^l a_{ir} = 0$ for all $i \in I$" is equivalent to the condition $p^l A_r = 0$, because of the above special choice of generators $B_i, i \in I$. Lemma is proved.

Corollary.

Proposition of n.3.6.2 is valid for $s = 1$.

Proof.

Let $\mathcal{J}$ be an ideal of $\mathcal{L}_{R,N,M}$ such that $\mathcal{J} \supset C_2(\mathcal{L}_{R,N,M})$ and $\mathcal{L}_{\mathcal{J}} = \mathcal{L}_{R,N,M}/\mathcal{J}$. Denote by $e_{\mathcal{J}}$ and $f_{\mathcal{J}}$ the images of $e_{R,N,M}$ and $f_{R,N,M}$ in $G(\mathcal{L}_{\mathcal{J},K_{tr}})$ and $G(\mathcal{L}_{\mathcal{J},K_{sep}})$, respectively. Then $e_{\mathcal{J}} = \sum_{r\in R} t^r D'_{r,0}$, where $D'_{r,0} = D_{r,0} \bmod \mathcal{J}_k$. Let $K(f_{\mathcal{J}})$ be the field of definition of $f_{\mathcal{J}}$ over K.

Now the above Proposition gives:

$$v(K(f_{\mathcal{J}})/K) < v_0 \Leftrightarrow \forall r \in R, \text{ if } rp^l \geq v_0, \text{ then } p^l D'_{r,0} = 0$$
$$\Longleftrightarrow \forall r \in R, \text{ if } rp^l \geq v_0, \text{ then } p^l D_{r,0} \in \mathcal{J} \otimes W_M(k)$$
$$\Longleftrightarrow \forall r \in R, \forall n \in \mathbb{Z}/N\mathbb{Z}, \text{ if } rp^l \geq v_0, \text{ then } p^l D_{r,n} \in \mathcal{J} \otimes W_M(k)$$

$\Longleftrightarrow$ $\mathcal{L}_{R,N,M,k}(v_0) \bmod C_2(\mathcal{L}_{R,N,M,k})$ is generated by the elements $p^l D_{r,n}$, where $r \in R, n \in \mathbb{Z}/N\mathbb{Z}$ and $p^l r \geq v_0$.

4.2. *Auxiliary construction.*

As earlier, $K = k((\tilde{t}_0)), N \geq 1, q = p^N$.

4.2.1. Let $r^* \in \mathbb{Q}^+(p)$ be such that $r^*(q-1) \in \mathbb{Z}$.

Following [A, n.6.3] introduce a separable extension K' of K such that

a) $[K' : K] = q$;

b) $K'K_{tr} = K_{tr}(T)$, where $T^q - T = \tilde{t}_0^{-r^*}$.

Herbrandt function of this extension is equal to

$$\phi_{K'/K}(x) = \begin{cases} x, & \text{for } 0 < x \leq r^* \\ r^* + \frac{x-r^*}{q}, & \text{for } x > r^*. \end{cases}$$

Remark. The graph of function $\phi_{K'/K}(x)$ has the unique edge point (r^*, r^*) (therefore $v(K'/K) = r^*$).

4.2.2. Let

$$E(x) = \exp(x + x^p/p + \dots + x^{p^n}/p^n + \dots) \in \mathbb{Z}_p[[x]]$$

be Artin-Hasse exponential.

Lemma. *There exists a uniformizer $\tilde{t}_0'$ of the field K' such that*

$$\tilde{t}_0'^q E\left(\frac{1}{r^*}\tilde{t}_0'^{r^*(q-1)}\right) = \tilde{t}_0.$$

Proof.

One can assume that $T = u^{-r^*}$ for some uniformizer u of K'. Therefore,

$$u^{-qr^*}(1 - u^{r^*(q-1)}) = \tilde{t}_0^{-r^*},$$
$$u^q(1 - u^{r^*(q-1)})^{-1/r^*} = \tilde{t}_0,$$
$$u^q(1 + \frac{1}{r^*}u^{r^*(q-1)}) \equiv \tilde{t}_0 \bmod (u^{q+2r^*(q-1)}O_{K'}).$$

Now Hensel Lemma gives the existence of $\tilde{t}_0' \in O_{K'}$ such that

$$\tilde{t}_0' \equiv u \bmod (u^{1+r^*(q-1)}O_{K'})$$

and

$$\tilde{t}_0'^q E\left(\frac{1}{r^*}\tilde{t}_0'^{r^*(q-1)}\right) = \tilde{t}_0,$$

q.e.d.

4.2.3. Clearly, $O_M(K') \supset O_M(K)$. Consider $\tilde{t} \in O_M(K)$ such that $\tilde{t} \bmod p = t_0$ and $\sigma\tilde{t} = \tilde{t}^p$ (c.f. n.3.4).

Lemma. *There exists* $\widetilde{t}' \in O_M(K')$ *such that* $\widetilde{t}' \bmod p = \widetilde{t_0}'$ *(c.f. n.4.2.2) and*

$$\widetilde{t}'^{q} E\left(\frac{1}{r^*}\widetilde{t}'^{r^*(q-1)}\right) = \widetilde{t}.$$

Proof.

This follows easily from Lemma of the above n.4.2.2 and Hensel Lemma.

4.2.4. Let $K'_M = k((\widetilde{t_0}'^{p^M}))$. Then K'_M is the subfield of K' and K' is a purely inseparable extension of K'_M of degree p^M.

As was mentioned in n.2.1, $O_M(K')$ can be identified with $\mathbb{Z}/p^{M+1}\mathbb{Z}$-algebra of Laurent series in the variable $\widetilde{t}'$ with coefficients in $W_M(k)$. Therefore, one can identify $O_M(K'_M)$ with the $\mathbb{Z}/p^{M+1}\mathbb{Z}$-subalgebra of $O_M(K')$ consisting of Laurent series in the variable $\widetilde{t_1} = \widetilde{t}'^{p^M}$. Clearly, $\widetilde{t_1} \bmod p$ is a uniformizer of K'_M and $\sigma\widetilde{t_1} = \widetilde{t_1}^p$ in $O_M(K'_M)$ (indeed, $\sigma\widetilde{t}' \equiv \widetilde{t}'^p \bmod pO_M(K')$, therefore, $\sigma\widetilde{t}'^{p^M} = \widetilde{t}'^{p^{M+1}}$ in $O_M(K')$).

4.2.5. Let $t_1 = \widetilde{t_1}^{-1} \in O_M(K'_M)$ and (as earlier) $t = \widetilde{t}^{-1} \in O_M(K)$.

Lemma.

$$t^{p^{2M}} = t_1^{qp^M} E\left(-\frac{1}{r^*}t_1^{-r^*p^M(q-1)}\right) \prod_{1\leqslant s\leqslant M} \exp\left(-\frac{1}{r^*}p^s t_1^{-r^*p^{M-s}(q-1)}\right).$$

Proof.

This equality is a formal consequence of Lemma of n.4.2.3 and of the following formulae: $E(x)^p = \exp(px)E(x^p)$, $E(x)^{p^{2M}} \equiv E(x^{p^M}) \bmod p^{M+1}$, $\widetilde{t}'^{-p^M} = t_1$ and $r^{*p^{M+s}} \equiv r^* \bmod p^{s+1}$ for $0 \le s \le M$.

4.3. *One reduction.*

4.3.1. Let $\mathcal{J} \subset \mathcal{L}_{R,N,M}$ be any ideal, $\mathcal{L}_{\mathcal{J}} = \mathcal{L}_{R,N,M}/\mathcal{J}$, $e_{\mathcal{J}}$ and $f_{\mathcal{J}}$ be the images of $e_{R,N,M}$ and $f_{R,N,M}$ under the maps

$$G(\mathcal{L}_{R,N,M,K_{tr}}) \longrightarrow G(\mathcal{L}_{\mathcal{J},K_{tr}})$$

and

$$G(\mathcal{L}_{R,N,M,K_{sep}}) \longrightarrow G(\mathcal{L}_{\mathcal{J},K_{sep}}),$$

respectively.

Let $K(f_{\mathcal{J}})$ be the field of definition of $f_{\mathcal{J}}$ over K and $K(\sigma^M f_{\mathcal{J}})$ be the field of definition of $\sigma^M f_{\mathcal{J}}$ over K. Then $K(f_{\mathcal{J}}) = K(\sigma^M f_{\mathcal{J}})$. This follows from the evident equivalence $e \underset{R}{\sim} \sigma^M e$ in $G(\mathcal{L}_{R,N,M,K_{tr}})$.

Let $K_M = k((\widetilde{t_0}^{p^M}))$. Then $K_M \subset K$ and K is purely inseparable extension of K_M of degree p^M. σ^M induces the isomorphism of fields $K \longrightarrow K_M$ which sends

$\widetilde{t}_0$ to $\widetilde{t}_0^{p^M}$. This isomorphism can be extended to the isomorphism $K_{sep}^{C_p(I)} \longrightarrow K_{M,sep}^{C_p(I)}$ by the following conditions $f_{R_1,N_1,M_1} \mapsto \sigma^M f_{R_1,N_1,M_1}$. Obviously, for any ideal $\mathcal{J} \subset \mathcal{L}_{R,N,M}$ there is an isomorphism of the extensions $K(\sigma^M f_{\mathcal{J}})/K$ and $K_M(\sigma^{2M} f_{\mathcal{J}})/K_M$ (here $K_M(\sigma^{2M} f_{\mathcal{J}})/K_M$ is the field of definition of $\sigma^{2M} f_{\mathcal{J}}$ over K_M).

So, for any ideal $\mathcal{J} \subset \mathcal{L}_{R,N,M}$ there is an equality of the largest upper ramification numbers

$$v(K(f_{\mathcal{J}})/K) = v(K_M(\sigma^{2M} f_{\mathcal{J}})/K_M).$$

Let

$$e'_{R,N,M} = \sum_{r \in R} t_1^r D_{r,0} \in G(\mathcal{L}_{R,N,M,K'_{M,tr}}),$$

and $f'_{R,N,M} \in G(\mathcal{L}_{R,N,M,K'_{M,sep}})$ be such that

$$\sigma f'_{R,N,M} = f'_{R,N,M} \circ e'_{R,N,M}$$

(the morphism σ on $O_M(K'_{M,K_{sep}})$ is given by the restriction of σ from $O_M(K')$ to $O_M(K'_M)$, c.f. n.4.2.4). As above, define for any ideal $\mathcal{J} \subset \mathcal{L}_{R,N,M}$ the element $f'_{\mathcal{J}} \in G(\mathcal{L}_{\mathcal{J},K'_{M,sep}})$. Then

$$v(K'_M(f'_{\mathcal{J}})/K'_M) = v(K'_M(\sigma^{M+N} f'_{\mathcal{J}})/K'_M).$$

4.3.2. Clearly, K'_M is separable over K_M, and one can define $X \in G(\mathcal{L}_{R,N,M,K_{M,sep}})$ from the equality

$$\sigma^{2M} f_{R,N,M} = \sigma^{M+N} f'_{R,N,M} \circ X.$$

Therefore, for the image $X_{\mathcal{J}}$ of X in $G(\mathcal{L}_{\mathcal{J},K_{M,sep}})$ one has

$$\sigma^{2M} f_{\mathcal{J}} = \sigma^{M+N} f'_{\mathcal{J}} \circ X_{\mathcal{J}}.$$

Proposition. *Let $v_0 \in \mathbb{Q}, v_0 > 0$, $\mathcal{J}$ be an ideal of $\mathcal{L}_{R,N,M}$ and $K'_M(X_{\mathcal{J}})$ be the field of definition of $X_{\mathcal{J}}$ over K'_M. If $r^* < v_0$, then*

$$v(K(f_{\mathcal{J}})/K) < v_0 \ \Leftrightarrow \ v(K'_M(X_{\mathcal{J}})/K_M) < v_0.$$

Proof.

We use the following lemma.

Lemma. *Let $v_{\mathcal{J}} = v(K(f_{\mathcal{J}})/K)$ and $v^*_{\mathcal{J}} = v(K'_M(f'_{\mathcal{J}})/K_M)$. Then either $v_{\mathcal{J}}$ and $v^*_{\mathcal{J}}$ are both $< v_0$, or $v^*_{\mathcal{J}} < v_{\mathcal{J}}$.*

Proof of Lemma.

We use arguments of [A, n.7.4].

The correspondence $t \mapsto t_1$ defines the isomorphism of fields

$$\alpha : K \longrightarrow K'_M.$$

This gives the isomorphism of liftings $O_M(K)$ and $O_M(K'_M)$. Since $\sigma t = t^p$ and $\sigma t_1 = t_1^p$, the correspondence $f_{\mathcal{J}} \mapsto f'_{\mathcal{J}}$ defines the extension of α to the isomorphism of fields

$$K(f_{\mathcal{J}}) \longrightarrow K'_M(f'_{\mathcal{J}}).$$

Let $\phi_1(x)$ and $\phi_2(x)$ be Herbrandt functions of the extensions $K(f_{\mathcal{J}})/K$ and $K'_M(f'_{\mathcal{J}})/K_M$, respectively. Then function $\phi_1(x)$ coincides with Herbrandt function of the extension $K'_M(f'_{\mathcal{J}})/K'_M$ and, therefore,

$$\phi_2(x) = \phi_{K'_M/K_M}(\phi_1(x)),$$

where $\phi_{K'_M/K_M}(x)$ is Herbrandt function of the extension K'_M/K_M.

On the one hand, $(\phi_1^{-1}(v_{\mathcal{J}}), v_{\mathcal{J}})$ and $(\phi_2^{-1}(v^*_{\mathcal{J}}), v^*_{\mathcal{J}})$ are the last edge points of the graphs of the functions $\phi_1(x)$ and $\phi_2(x)$, respectively. On the other hand, $\phi_{K'_M/K_M}$ coincides with Herbrandt function of the extension K'/K, c.f. n.4.2.1.

Therefore,

$$v^*_{\mathcal{J}} = \max\{\ r^*,\ r^* + \frac{v_{\mathcal{J}} - r^*}{q}\ \}.$$

Now, if $v_{\mathcal{J}} \leq r^*$, then $v^*_{\mathcal{J}} \leq r^*$ and, in this case, $v_{\mathcal{J}}$ and $v^*_{\mathcal{J}}$ are both $< v_0$.

If $v_{\mathcal{J}} > r^*$, then

$$v^*_{\mathcal{J}} = r^* + \frac{v_{\mathcal{J}} - r^*}{q} < v_{\mathcal{J}},$$

q.e.d.

Continue the proof of our Proposition.

It follows from the definition of $X_{\mathcal{J}}$ that

$$K'_M(X_{\mathcal{J}}) \subset K'_M(\sigma^{2M} f_{\mathcal{J}}) K'_M(\sigma^{M+N} f'_{\mathcal{J}}).$$

By arguments of n.4.3.1 one has (in notation of the above Lemma)

$$v(K'_M(X_{\mathcal{J}})/K_M) \leq \max\{\ v_{\mathcal{J}}, v^*_{\mathcal{J}}\ \}.$$

Obviously, the above Lemma gives the implication

$$v(K(f_{\mathcal{J}})/K) < v_0 \implies v(K'_M(X_{\mathcal{J}})/K_M) < v_0.$$

The inverse implication can be obtained similarly. Indeed, let $v(K'_M(X_{\mathcal{J}})/K_M) < v_0$ and $v_{\mathcal{J}} \geq v_0$. One has from the definition of $X_{\mathcal{J}}$

$$v_{\mathcal{J}} \leq \max\{v^*_{\mathcal{J}}, v(K'_M(X_{\mathcal{J}})/K_M)\}.$$

Therefore, $v_0 \leq v_{\mathcal{J}} \leq v^*_{\mathcal{J}}$, but this is impossible because of our Lemma.

4.3.3. Corollary. *If $r^* < v_0$ and $1 \leq s < p$, then $\mathcal{L}_{R,N,M}(v_0) + C_{s+1}(\mathcal{L}_{R,N,M})$ is the minimal element in the family of ideals $\mathcal{J}$ of $\mathcal{L}_{R,N,M}$, such that*

a) $\mathcal{J} \supset C_{s+1}(\mathcal{L}_{R,N,M})$;

b) $v(K'_M(X_{\mathcal{J}})/K_M) < v_0$.

4.4. *Some calculations.*

Let $v_0 \in \mathbb{Q}, v_0 > 0$, R be a finite subset in $\mathbb{Q}^+(p)$ and M be a nonnegative integer.

For any natural number N we use the notation $q = p^N$.

4.4.1. Lemma. *There exists a natural number* $N_2(R, M, v_0)$ *such that for any* $N \geqslant N_2(R, M, v_0)$ *there exist* $r^* = r^*(N, R, M, v_0) \in \mathbb{Q}^+(p)$ *and* $a^* = a^*(N, R, M, v_0) \in \mathbb{Q}^+(p)$ *such that*

a) $r^* < v_0$;

b) $r^*(q-1) \in \mathbb{N}$;

c) if $r \in R, r < v_0$, *then* $qp^M r - qa^* \leqslant -a^*$;

d) if $r \in R$ *and* $p^i r < v_0$ *for some* $i \in \mathbb{Z}, i \geqslant 0$, *then*

$$qp^i r - r^*(q-1) \leqslant -a^*;$$

e) if $p^i(r_1 + \frac{r_2}{p^n}) < v_0$ *for some* $r_1, r_2 \in R$ *and integers* $i, n \geqslant 0$, *then*

$$qp^i(r_1 + \frac{r_2}{p^n}) - (q-1)r^* < 0.$$

Proof.

Let $\delta_1 = \delta_1(R, v_0)$ be the minimum of all positive values of the expression $v_0 - p^i r$, where $i \in \mathbb{Z}, i \geq 0$ and $r \in R$.

Let $\delta_2 = \delta_2(R, v_0)$ be the minimum of all positive values of the expression

$$v_0 - p^i \left(r_1 + \frac{r_2}{p^n}\right),$$

where i, n are nonnegative integers and $r_1, r_2 \in R$.

Clearly, δ_1 and δ_2 exist and $0 < \delta_2 \leqslant \delta_1$.

Take a natural number $N_2 = N_2(R, M, v_0)$ such that for $q_2 = p^{N_2}$ and

$$\widetilde{v_0} = \max\left\{\frac{q_2 + 2p^M}{q_2 - 1}(v_0 - \delta_1), \frac{q_2}{q_2 - 1}(v_0 - \delta_2)\right\}$$

one has the following inequality

$$v_0 - \widetilde{v_0} > \frac{2}{q_2 - 1}.$$

If $N \geq N_2$, then for

$$v = \max\left\{\frac{q + 2p^M}{q - 1}(v_0 - \delta_1), \frac{q}{q - 1}(v_0 - \delta_2)\right\}$$

one has

$$v - v_0 \geq v_0 - \widetilde{v_0} > \frac{2}{q_2 - 1} \geq \frac{2}{q - 1}.$$

Therefore, there exists $m \in \mathbb{N}$ such that

$$\frac{m}{q-1}, \frac{m+1}{q-1} \in (v, v_0).$$

At least one of these two fractions should be an element of $\mathbb{Q}^+(p)$ which we shall denote by r^*.

Clearly, the requirements a) and b) of our Lemma are satisfied.

If $r_1, r_2 \in R, i, n \geq 0$ and $p^i(r_1 + \frac{r_2}{p^n}) < v_0$, then

$$qp^i\left(r_1 + \frac{r_2}{p^n}\right) - (q-1)r^* < q(v_0 - \delta_2) - (q-1)v \leq 0$$

(c.f. the above definition of v) and the requirement e) is also valid.

Let $a^* \in \mathbb{Q}^+(p)$ be such that

$$\frac{q}{q-1}p^M(v_0 - \delta_1) \leq a^* \leq 2p^M(v_0 - \delta_1).$$

If $r \in R, r < v_0$, then $r \leq v_0 - \delta_1$ and

$$qp^M r \leq qp^M(v_0 - \delta_1) \leq (q-1)a^*,$$

therefore, c) is valid.

If $r \in R$ and $p^i r < v_0$ for some $i \geq 0$, then $p^i r \leq v_0 - \delta_1$ and the requirement d) is obtained as follows

$$qp^i r - r^*(q-1) \leq q(v_0 - \delta_1) - v(q-1) \leq q(v_0 - \delta_1) - (q + 2p^M)(v_0 - \delta_1) \leq -a^*.$$

Lemma is proved.

4.4.2. For fixed v_0, R, M and a natural number $N \geq N_2(R, M, v_0)$ we use until the end of n.4 the following more simple notation:

$L = \mathcal{L}_{R,N,M}$ and analogously $L_k = \mathcal{L}_{R,N,M,k}, L_{tr} = \mathcal{L}_{R,N,M,K'_{M,tr}}, L_{sep} = \mathcal{L}_{R,N,M,K'_{M,sep}}$;

$L(v_0) = \mathcal{L}_{R,N,M}(v_0)$ and analogously $L(v_0)_{sep} = \mathcal{L}_{R,N,M,K'_{M,sep}}(v_0)$;

$\widetilde{D}_{r,0} = D_{r,2M}$ for any $r \in R$;

$E = \sigma^{2M} e_{R,N,M} = \sum_{r \in R} t^{rp^{2M}} \widetilde{D}_{r,0}$ and $E_1 = \sigma^M e'_{R,N,M} = \sum_{r \in R} t_1^{rp^M} \widetilde{D}_{r,0}$;

$F = \sigma^{2M} f_{R,N,M} \in L_{sep}$ and $F_1 = \sigma^M f'_{R,N,M} \in L_{sep}$.

$\widetilde{\mathcal{F}}(\gamma, 0) = \mathcal{F}_{R,N,M}(\gamma, 2M) \bmod C_3(L_k) =$

$$= \sum_{\substack{r \in R, i \geqslant 0 \\ rp^i = \gamma}} rp^i \widetilde{D}_{r,i} - \sum_{\substack{r_1, r_2 \in R \\ 0 \leqslant n < N, i \geqslant 0 \\ p^i(r_1 + \frac{r_2}{p^n}) = \gamma}} \widetilde{\eta}(n, 0) r_1 p^i [\widetilde{D}_{r_1,i}, \widetilde{D}_{r_2,i-n}].$$

Denote by $W_M(k)\{\widetilde{t_1}\}$ the $W_M(k)$-algebra of Laurent series in one variable $\widetilde{t_1}$. Then $O_M(K'_M) \simeq W_M(k)\{\widetilde{t_1}\}$ and

$$O_M(K'_{M,tr}) = \varinjlim_{(n,p)=1} W_M(k)\{\widetilde{t_1}^{1/n}\}.$$

Consider its subalgebra of "power series"

$$O'_{M,tr} := \varinjlim_{(n,p)=1} W_M(k)[[\widetilde{t_1}^{1/n}]].$$

This subalgebra can be identified with a lifting of the valuation ring $O_{K'_{M,tr}}$ of the field $K'_{M,tr}$ modulo p^{M+1}.

We also use more simple notation $\mathcal{O}'(L_{tr})$ for the Lie $O'_{M,tr}$-algebra $L \otimes O'_{M,tr}$.

Inductive assumption.

One can assume that Proposition 3.6.2 is valid (for $s = 2$) for the Lie algebra $\mathcal{L}_{R,N,M-1}$, where $N \geq N_2(R, M-1, v_0)$. As

$$N_2(R, M, v_0) \geq N_2(R, M-1, v_0),$$

we can assume that for $N \geq N_2(R, M, v_0)$ the ideal

$$L(v_0)_k \operatorname{mod}(p^M L_k + C_3(L_k))$$

of the Lie algebra $L_k \operatorname{mod}(p^M L_k + C_3(L_k))$ is generated by the elements

$$\sigma^n \widetilde{\mathcal{F}}(\gamma, 0) \operatorname{mod} p^M L_k + C_3(L_k),$$

where $n \in \mathbb{Z}/N\mathbb{Z}, \gamma \geq v_0$.

4.4.3. Let $\Delta_1 \in L_{tr}$ be such that $E = \sigma^N E_1 + \Delta_1$. Then (c.f. n.4.2.5)

$$\Delta_1 = \sum_{r \in R} t_1^{qrp^M} (\mathcal{E}^r - 1) \widetilde{D}_{r,0},$$

where

$$\mathcal{E} = E\left(-\frac{1}{r^*} t_1^{-r^* p^M (q-1)}\right) \prod_{1 \leqslant s \leqslant M} \exp\left(-\frac{1}{r^*} p^s t_1^{-r^* p^{M-s}(q-1)}\right).$$

As in n.4.3, consider $X \in L_{sep}$ such that $F = \sigma^N F_1 \circ X$. Obviously,

$$\sigma X - X = \Delta_1 \operatorname{mod} C_2(L_{sep}).$$

Proposition.

a) $\Delta_1 \in L(v_0)_{sep} + t_1^{-a^*} \mathcal{O}'(L_{tr}) + C_2(L_{sep})$;

b) $[X, \sigma^N E_1] \equiv$

$$\equiv - \sum_{0 \leqslant n < N} [\sigma^n \Delta_1, \sigma^N E_1] \operatorname{mod} \left([L(v_0)_{sep}, L_{sep}] + t_1^{-a^*} \mathcal{O}'(L_{tr}) + C_3(L_{sep})\right).$$

Proof.

Let

$$\mathcal{E}_s = \exp\left(-\frac{1}{r^*} p^s t_1^{-r^* p^{M-s}(q-1)}\right)$$

for $1 \leq s \leq M$ and

$$\mathcal{E}_0 = E\left(-\frac{1}{r^*} t_1^{-r^* p^M (q-1)}\right).$$

Lemma. *For any $r \in R$ and $0 \le s \le M$ one has*

$$t_1^{qrp^M}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0} \in L(v_0)_{sep} + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_2(L_{sep}).$$

Proof of lemma.

Let $rp^s \geqslant v_0$. Then

$$p^s\widetilde{D}_{r,0} \in L(v_0)_k + C_2(L_k),$$

c.f. n.4.1. Therefore, if $s = 0$, then

$$t_1^{qrp^M}(\mathcal{E}_0^r - 1)\widetilde{D}_{r,0} \in L(v_0)_{sep} + C_2(L_{sep}).$$

If $1 \leqslant s \leqslant M$, then

$$\mathcal{E}_s^r - 1 = \exp\left(-\frac{r}{r^*}p^s t_1^{-r^*p^{M-s}(q-1)}\right) - 1 \in p^s O_M(K'_{M,sep})$$

and again

$$t_1^{qrp^M}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0} \in L(v_0)_{sep} + C_2(L_{sep}).$$

Let $rp^s < v_0$. If $1 \leqslant s \leqslant M$, then

$$t_1^{qrp^M}(\mathcal{E}_s^r - 1) = t_1^{qrp^M}\left[\exp\left(-\frac{r}{r^*}p^s t_1^{-r^*p^{M-s}(q-1)}\right) - 1\right] \in$$

$$\in t_1^{qrp^M - r^*p^{M-s}(q-1)}O'_{M,tr} \subset t_1^{-p^{M-s}a^*}O'_{M,tr} \subset t_1^{-a^*}O'_{M,tr}$$

(we use the inequality d) of Lemma 4.4.1).

This means that

$$t_1^{qrp^M}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0} \in t_1^{-a^*}\mathcal{O}'(L_{tr}).$$

If $s = 0$, then

$$\mathcal{E}_0^r - 1 \equiv \left\{\widetilde{\exp}\left(-\frac{r}{r^*}t_1^{-r^*p^M(q-1)}\right) - 1\right\} \bmod t_1^{-r^*p^{M+1}(q-1)}O'_{M,tr}.$$

As $r < v_0$, the enequality d) of Lemma 4.4.1 gives that

$$t_1^{qrp^M}(\mathcal{E}_0^r - 1) \in t_1^{qrp^M - r^*p^M(q-1)}O'_{M,tr} \subset t_1^{-p^M a^*}O'_{M,tr} \subset t_1^{-a^*}O'_{M,tr}$$

and, therefore, $t_1^{qrp^M}(\mathcal{E}_0^r - 1)\widetilde{D}_{r,0} \in t_1^{-a^*}O'_{M,tr}$.

Lemma is proved.

Continue the proof of our Proposition.

a) As $\prod_{s<i\leqslant M}\mathcal{E}_i^r \in O'_{M,tr}$, the above Lemma gives

$$\Delta_1 = \sum_{\substack{r\in R\\ 0\le s\le M}}\left[t_1^{qrp^M}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0}\prod_{s<i\le M}\mathcal{E}_i^r\right] \in L(v_0)_{sep} + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_2(L_{sep}).$$

b) From n.a) it follows that for $n \geqslant N$

$$\sigma^n \Delta_1 \in L(v_0)_{sep} + t_1^{-qa^*} \mathcal{O}'(L_{tr}) + C_2(L_{sep}).$$

Then

$$\sigma^N E_1 = \sum_{r \in R} t_1^{qrp^M} \widetilde{D}_{r,0} \equiv \sum_{\substack{r \in R \\ r < v_0}} t_1^{qrp^M} \widetilde{D}_{r,0} \operatorname{mod} L(v_0)_{sep} + C_2(L_{sep}),$$

because $\widetilde{D}_{r,0} \in L(v_0)_k + C_2(L_k)$ for $r \geqslant v_0$.

With respect to c) of Lemma 4.4.1, $qrp^M \leqslant (q-1)a^*$ for $r < v_0$, therefore,

$$\sigma^N E_1 \in L(v_0)_{sep} + t_1^{(q-1)a^*} \mathcal{O}'(L_{tr}) + C_2(L_{sep}).$$

So, for $n \geqslant N$

$$[\sigma^n \Delta_1, \sigma^N E_1] \in L(v_0)_{sep} + t_1^{-a^*} \mathcal{O}'(L_{tr}) + C_3(L_{sep}).$$

In order to finish the proof one needs only remark that

$$X \equiv -\sum_{n \geqslant 0} \sigma^n \Delta_1 \operatorname{mod}(L(v_0)_{sep} + C_2(L_{sep})),$$

by the part a) of our Proposition, which was proved earlier.

Proposition is proved.

4.4.4. Let $\Delta \in G(L_{tr})$ be such that $E = \sigma^N E_1 \circ \Delta$. Then

$$\Delta \equiv \Delta_1 - \frac{1}{2}[\sigma^N E_1, \Delta_1] \operatorname{mod} C_3(L_{sep}).$$

Applying σ to the both sides of the equality $F = \sigma^N F_1 \circ X$, one gets

$$\sigma F = F \circ E = \sigma^N F_1 \circ X \circ \sigma^N E_1 \circ \Delta$$

and

$$\sigma(\sigma^N F_1 \circ X) = \sigma^N F_1 \circ \sigma^N E_1 \circ \sigma X.$$

Therefore,

$$\sigma X = X \circ \{X, \sigma^N E_1\} \circ \Delta,$$

where $\{\ ,\ \}$ is a commutator in the group $G(L_{sep})$.

Obviously,

$$\{X, \sigma^N E_1\} \equiv [X, \sigma^N E_1] \operatorname{mod} C_3(L_{sep})$$

and by n.b) of Proposition n.4.4.3 one has

$$\{X, \sigma^N E_1\} \equiv$$

$$\equiv - \sum_{0\leqslant n<N} [\sigma^n\Delta_1, \sigma^N E_1] \bmod \left([L(v_0)_{sep}, L_{sep}] + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_3(L_{sep})\right).$$

Proceeding in the same way we obtain

$$X \circ \Delta = X + \Delta + \frac{1}{2}[X, \Delta] \equiv$$

$$\equiv X + \Delta_1 - \frac{1}{2}[\sigma^N E_1, \Delta_1] + \frac{1}{2}[X, \Delta_1] \equiv X + \Delta_1 - \frac{1}{2}[\sigma^N E_1, \Delta_1]$$

$$\bmod \left([L(v_0)_{sep}, L_{sep}] + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_3(L_{sep})\right),$$

because X and Δ_1 are in $L(v_0)_{sep} + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_2(L_{sep})$, c.f. n.4.4.3.

Therefore,

$$\sigma X - X \equiv \Delta_1 - \frac{1}{2}[\sigma^N E_1, \Delta_1] + [X, \sigma^N E_1] \equiv$$

$$\equiv \Delta_1 - \sum_{0\leqslant n<N} \widetilde{\eta}(n,0)\sigma^n[\Delta_1, \sigma^{N-n}E_1]$$

$$\bmod \left([L(v_0)_{sep}, L_{sep}] + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_3(L_{sep})\right),$$

where

$$\widetilde{\eta}(n,0) = \begin{cases} 1, & \text{if } 0 < n < N \\ 1/2, & \text{if } n = 0. \end{cases}$$

4.4.5. Proposition.

$$\Delta_1 \equiv \sum_{\substack{r\in R \\ 0\leqslant s\leqslant M}} t_1^{qrp^M}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0}$$

$$\bmod \left(pL(v_0)_{sep} + [L(v_0)_{sep}, L_{sep}] + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_3(L_{sep})\right).$$

Proof.

We use notation of n.4.4.3. Let $r \in R$ and $0 \leq s \leq M$.

a) If $p^s r < v_0$, then

$$t_1^{qp^M r}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0} \in t_1^{-a^*}\mathcal{O}'(L_{tr}),$$

c.f. proof of Lemma n.4.4.3.

b) If $s \geq 1$ and $p^s r \geq pv_0$, then

$$t_1^{qp^M r}(\mathcal{E}_s^r - 1)\widetilde{D}_{r,0} \in pL(v_0)_{sep} + [L(v_0)_{sep}, L_{sep}] + C_3(L_{sep}).$$

This is implied by the following Lemma.

Lemma. *If $r \in R$, $i \geq 0, i \in \mathbb{Z}$ and $p^i r \geq v_0$, then*

$$p^{i+1}\widetilde{D}_{r,0} \in pL(v_0)_k + [L(v_0)_k, L_k] + C_3(L_k).$$

Proof of Lemma.

By the inductive assumption of n.4.4.2 one has

$$\widetilde{\mathcal{F}}(p^i r, 0) = p^i r \widetilde{D}_{r,i} - \sum_{\substack{r_1, r_2 \in R \\ 0 \leqslant n < N, i_1 \geqslant 0 \\ p^{i_1}(r_1 + \frac{r_2}{p^n}) = p^i r}} \widetilde{\eta}(n,0) p^{i_1} r_1 [D_{r_1,i_1}, D_{r_2,i_1-n}] \in L(v_0)_k + p^M L_k + C_3(L_k).$$

Therefore, $p\widetilde{\mathcal{F}}(p^i r, 0) \in pL(v_0)_k + C_3(L_k)$.
If the summand

$$p^{i_1+1}\widetilde{\eta}(n,0) r_1 [D_{r_1,i_1}, D_{r_2,i_1-n}]$$

appears in the expression of $p\widetilde{\mathcal{F}}(p^i r, 0)$, then it belongs to $[L(v_0)_k, L_k] + C_3(L_k)$.

Indeed, at least one of two numbers $p^{i_1+1} r_1$ and $p^{i_1+1} r_2$ should be $\geq v_0$ (otherwise, $p^{i_1}(r_1 + \frac{r_2}{p^n}) < \frac{2v_0}{p} < v_0$). Therefore, $p^{i_1+1}\widetilde{D}_{r_1,i_1}$ or $p^{i_1+1}\widetilde{D}_{r_2,i_1-n}$ belongs to $L(v_0)_k + C_2(L_k)$.

Lemma is proved.

Now our Proposition follows from the identity

$$\prod_{0 \leqslant s \leqslant M} \mathcal{E}_s^r - 1 = \prod_{\substack{1 \leqslant l \leqslant M \\ 0 \leqslant s_1 < \ldots < s_l \leqslant M}} (\mathcal{E}_{s_1}^r - 1) \ldots (\mathcal{E}_{s_l}^r - 1).$$

4.4.6. Proposition. *Let δ_1 be a rational number from the proof of Lemma 4.4.1. Then*

$$\sum_{0 \leq n < N} \widetilde{\eta}(n,0) \sigma^n [\Delta_1, \sigma^{N-n} E_1] \equiv \sum_{\substack{r_1, r_2 \in R \\ 0 \leqslant n < N, 0 \leqslant s \leqslant M \\ v_0 \leqslant p^s (r_1 + \frac{r_2}{p^n}) \leqslant 2(v_0 - \delta_1)}} \widetilde{\eta}(n,o) t_1^{q(r_1 + \frac{r_2}{p^n}) p^M} (\mathcal{E}_s^{r_1} - 1) [\widetilde{D}_{r_1,0}, \widetilde{D}_{r_2,-n}]$$

$$\bmod \left([L(v_0)_{sep}, L_{sep}] + t_1^{-a^*} \mathcal{O}'(L_{tr}) + C_3(L_{sep}) \right).$$

Proof.

Indeed,

$$\sum_{0 \leqslant n < N} \widetilde{\eta}(n,0) \sigma^n [\Delta_1, \sigma^{N-n} E_1] =$$

$$= \sum_{0 \leqslant n < N} \widetilde{\eta}(n,0) \sigma^n \left[\sum_{r_1} t_1^{q r_1 p^M} (\mathcal{E}_0^{r_1} \ldots \mathcal{E}_M^{r_1} - 1) \widetilde{D}_{r_1,0}, \sum_{r_2} t_1^{r_2 p^{M+N-n}} \widetilde{D}_{r_2,-n} \right] =$$

$$= \sum_{\substack{r_1, r_2 \\ 0 \leqslant n < N}} \widetilde{\eta}(n,0) t_1^{q(r_1+\frac{r_2}{p^n})p^M} (\mathcal{E}_0^{r_1} \dots \mathcal{E}_M^{r_1} - 1)[\widetilde{D}_{r_1,0}, \widetilde{D}_{r_2,-n}].$$

Then, as in n.4.4.5, we obtain

a) If $p^s(r_1 + \frac{r_2}{p^n}) < v_0$, then

$$t_1^{qp^M(r_1+\frac{r_2}{p^n})}(\mathcal{E}_s^{r_1} - 1)[\widetilde{D}_{r_1,0}, \widetilde{D}_{r_2,-n}] \in t_1^{-a^*} \mathcal{O}'(L_{tr}).$$

b) If $p^s(r_1 + \frac{r_2}{p^n}) > 2(v_0 - \delta_1)$, then either $p^s r_1 > v_0 - \delta_1$, or $p^s r_2 > v_0 - \delta_1$. Let, for example, $p^s r_1 > v_0 - \delta_1$. Then $p^s r_1 \geqslant v_0$, it gives

$$p^s \widetilde{D}_{r_1,0} \in L(v_0)_k + C_2(L_k)$$

and, therefore,

$$p^s[\widetilde{D}_{r_1,0}, \widetilde{D}_{r_2,-n}] \in [L(v_0)_k, L_k] + C_3(L_k).$$

Remark, that $\mathcal{E}_s^{r_1} - 1 \equiv 0 \bmod p^s$.

Now one can finish the proof of our Proposition in the same way as it was done in the proof of Proposition n.4.4.5.

4.4.7. Proposition.

$$\Delta_1 - \sum_{0 \leqslant n < N} \widetilde{\eta}(n,0)\sigma^n[\Delta_1, \sigma^{N-n}E_1] \equiv$$

$$\equiv -\frac{1}{r^*} \sum_{\substack{r \in R \\ 0 \leqslant s \leqslant M}} r p^s \left[t_1^{qrp^s - r^*(q-1)}\right]^{p^{M-s}} \widetilde{D}_{r,0} +$$

$$+\frac{1}{r^*} \sum_{\substack{r_1, r_2 \in R \\ 0 \leqslant s \leqslant M \\ 0 \leqslant n < N}} r_1 p^s \widetilde{\eta}(n,0) \left[t_1^{q(r_1+\frac{r_2}{p^n})p^s - r^*(q-1)}\right]^{p^{M-s}} [\widetilde{D}_{r_1,0}, \widetilde{D}_{r_2,-n}]$$

$$\bmod pL(v_0)_{sep} + [L(v_0)_{sep}, L_{sep}] + t_1^{-a^*}\mathcal{O}'(L_{tr}) + C_3(L_{sep}).$$

Proof.

It is easy to see that the changement of $\mathcal{E}_s^{r_1} - 1$ by the first member $-\frac{r_1}{r^*} t_1^{-r^*(q-1)p^{M-s}}$ of its expansion in powers of t_1 does not affect the expression for

$$\sum_{0 \leqslant n < N} \widetilde{\eta}(n,0)\sigma^n[\Delta_1, \sigma^{N-n}E_1]$$

from Proposition 4.4.6 modulo $t_1^{-a^*}\mathcal{O}'(L_{tr})$. In order to finish the proof one needs only show that this procedure can be done with the expression of Δ_1 from the Proposition 4.4.5. This is implied by the following lemma.

Lemma. *If* $r \in R, p^s r > 2(v_0 - \delta_1)$, *then* $p^s \widetilde{D}_{r,0} \in L(v_0)_k + C_3(L_k)$.

Proof.

Let $p^{s_1} r_1$ be the largest number such that $r_1 \in R, p^{s_1} r_1 > 2(v_0 - \delta_1)$ and

$$p^{s_1} \widetilde{D}_{r_1,0} \notin L(v_0)_k + C_3(L_k).$$

From inductive assumption it follows that

$$p^{s_1} \widetilde{D}_{r_1,0} \in L(v_0)_k + +p^M L_k + C_3(L_k).$$

Further, in the expansion

$$\Delta_1 - \sum_{0 \leqslant n < N} \widetilde{\eta}(n,0)\sigma^n[\Delta_1, \sigma^{N-n} E_1] = \sum_{\substack{\gamma_1 \in \mathbf{Z}^+(p) \\ m \in \mathbf{Z}, m \geqslant 0}} t_1^{\gamma_1 p^m} A_{\gamma_1, m},$$

where all $A_{\gamma_1,m} \in L_k$, one has

1) $A_{\gamma_1,m} \in L(v_0)_k + C_3(L_k)$ for $\gamma_1 > qp^{s_1} r_1 - r^*(q-1)$;

2) $A_{\gamma_1,m} \in L(v_0)_k + C_3(L_k)$ for $\gamma_1 = qp^{s_1} r_1 - r^*(q-1), m \neq M - s_1$.

Therefore, if $K'_M(X_{L(v_0)})$ is the field of definition of

$$X \bmod L(v_0)_{sep} + C_3(L_{sep}),$$

then the largest upper ramification number $v(K'_M(X_{L(v_0)})/K'_M)$ is equal to γ_1 and, therefore,

$$v(K'_M(X_{L(v_0)})/K_M) = \frac{\gamma_1 - r^*}{q} + r^* = p^{s_1} r_1.$$

But the inequality $p^{s_1} r_1 > 2(v_0 - \delta_1) \geqslant v_0 - \delta_1$ implies the inequality $p^{s_1} r_1 \geqslant v_0$. This is impossible because of $v(K'_M(X_{L(v_0)})/K_M) < v_0$.

This contradiction proves our Lemma.

4.4.8. It is easy to see that for any ideal J of the Lie algebra L such that

$$J \supset pL(v_0) + [L(v_0), L] + C_3(L),$$

the field of definition of $X \bmod J_{sep}$ coincides with the field of definition of $Y \bmod J_{sep}$, where $Y \in L_{sep}$ and satisfies the equation

$$\sigma Y - Y = \sum_{\substack{r \in R \\ 0 \leqslant s \leqslant M}} r p^s t_1^{qrp^s - r^*(q-1)} \widetilde{D}_{r,s} -$$

$$- \sum_{\substack{r_1, r_2 \in R \\ 0 \leqslant s \leqslant M \\ 0 \leqslant n < N}} r_1 p^s \widetilde{\eta}(n,0) t_1^{q(r_1 + \frac{r_2}{p^n})p^s - r^*(q-1)} [\widetilde{D}_{r_1,s}, \widetilde{D}_{r_2,s-n}].$$

So,

$$\sigma Y - Y = \sum_{\gamma \in \mathbf{Q}, \gamma > 0} t_1^{q\gamma - r^*(q-1)} \widetilde{\mathcal{F}}(\gamma, 0),$$

c.f. n.4.4.2.

4.5. *The end of the proof of theorem.*

Let $J_0 = \mathcal{L}_{R,N,M}^{(v_0)}$. We must prove, that

$$J_0 + C_3(L) = L(v_0) + C_3(L).$$

From n.4.4.1 it follows that

$$J_0 \operatorname{mod} C_2(L) = L(v_0) \operatorname{mod} C_2(L).$$

By the induction assumption one has

$$J_0 \operatorname{mod}(p^M L + C_3(L)) = L(v_0) \operatorname{mod}(p^M L + C_3(L)).$$

Therefore,

$$J_{0,K'_{M,sep}} \supset pL(v_0)_{sep} + [L(v_0)_{sep}, L_{sep}] + C_3(L_{sep}).$$

Now the last formula of n.4.4.8 gives that

$$K'_M(X_{J_0}) \subset K'_{M,tr},$$

and therefore

$$J_0 \operatorname{mod} C_3(L) \supset L(v_0) \operatorname{mod} C_3(L).$$

Conversely, let

$$\gamma_0 = \max\{\ \gamma \in \mathbb{Q}\ \mid\ \gamma \geq v_0,\ \widetilde{\mathcal{F}}_{\gamma,0} \notin L(v_0)_k\ \}.$$

Now the last formula of n.4.4.8 and Lemma n.4.1 give

$$v(K'_M(X_{L(v_0)})/K'_M) = q\gamma_0 - r^*(q-1).$$

Now the following inequality

$$v(K'_M(X_{L(v_0)})/K_M) = \frac{q\gamma_0 - r^*(q-1) - r^*}{q} + r^* = \gamma_0 \geq v_0$$

gives the contradiction to the Corollary of n.4.3.3.

Theorem of n.3.4 is proved (modulo 3-rd commutators).

5. The case of a local field with finite residue field.

Let N_0 be a fixed natural number, K_0 be a complete discrete valuation field of characteristic $p > 0$ with finite residue field $\mathbb{F}_{q_0}$, where $q_0 = p^{N_0}$. Fix a uniformizer $\widetilde{t_0}$ of the field K_0, then a fixed embedding $\mathbb{F}_{q_0} \subset k = \bar{\mathbb{F}}_p$ defines the embedding $K_0 = \mathbb{F}_{q_0}((\widetilde{t_0})) \subset K$, where $K = k((\widetilde{t_0}))$ is a local field from n.2.1.

Let $\Gamma = \operatorname{Gal}(K_{sep}/K_0)$, $\Gamma_0 = \operatorname{Gal}(K_{sep}/K_0)$ and $\Gamma_0(p)$ (respectively, $\Gamma(p)$) be the Galois group of the maximal p-extension of the field K_0 (respectively, of the field K) in $K_{0,sep} = K_{sep}$.

In n.5.1 we apply the generalisation of Artin-Schreier theory from n.1 to the construction of an identification

$$\bar{\psi}^{\circ} : \Gamma_0(p)/C_p(\Gamma_0(p)) \simeq G(L),$$

where $L = \widetilde{L}/C_p(\widetilde{L})$, and $\widetilde{L}$ is a free pro-p-algebra Lie over $\mathbb{Z}_p$.

In n.5.2 we describe (in the terms of the identification $\bar{\psi}^0$) the action of the Galois group $\mathrm{Gal}(K_0/\mathbb{F}_p((\widetilde{t_0}))\ )$ on $\Gamma_0(p)/C_p(\Gamma_0(p))$ by conjugation.

Let

$$\bar{\psi}(p) : \Gamma(p)/C_p(\Gamma(p)) \simeq G(\mathcal{L}(p))$$

be the identification from n.3.5.2. Consider the homomorphism of groups

$$\gamma : \Gamma(p)/C_p(\Gamma(p)) \longrightarrow \Gamma_0(p)/C_p(\Gamma_0(p)),$$

defined by the imbedding $\Gamma \subset \Gamma_0$. With respect to the identifications $\bar{\psi}^{\circ}$ and $\bar{\psi}(p)$ the homomorphism γ can be described in the terms of some morphism of Lie $\mathbb{Z}_p$-algebras

$$\delta : \mathcal{L}(p) \longrightarrow L.$$

In nn.5.3-5.4 we give an explicit construction of this morphism.

Let $\{\mathcal{L}(p)^{(v)}\}_{v>0}$ and $\{L^{(v)}\}_{v>0}$ be the filtrations of the Lie algebras $\mathcal{L}(p)$ and L, corresponding to the ramification filtrations $\{\Gamma(p)^{(v)}\}_{v>0}$ and $\{\Gamma_0(p)^{(v)}\}_{v>0}$, respectively. For any $v \in \mathbb{Q}, v > 0$, the equality $\Gamma(p)^{(v)} = \Gamma_0(p)^{(v)}$ implies the equality $\delta(\mathcal{L}(p)^{(v)}) = L^{(v)}$. Therefore, the explicit construction of δ with the description of the filtration $\{\mathcal{L}(p)^{(v)}\}_{v>0}$ from n.3.5.3 permit us to give in n.5.5 a description of the image of the ramification filtration of the group Γ_0 in $\Gamma_0(p)/C_p(\Gamma_0(p))$.

5.1. *Construction of identification* $\bar{\psi}^{\circ}$.

As earlier, let

$$\mathbb{Z}^+(p) = \{\ a \in \mathbb{N} \mid (a,p) = 1\ \}.$$

For any finite subset $A \subset \mathbb{Z}^+(p)$ and an integer $M \geqslant 0$ introduce the free Lie $\mathbb{Z}/p^{M+1}\mathbb{Z}$ -algebra $\widetilde{L}_{A,M}$ with the module of free generators

$$\underset{a\in A}{\oplus} \mathrm{Hom}(W_M(\mathbb{F}_{q_0}), W_M(\mathbb{F}_p))_a \oplus W_M(\mathbb{F}_p)\widetilde{V}_0.$$

The system $\{\widetilde{L}_{A,M}\}$ is a projective system of Lie algebras with respect to connecting morphisms $\widetilde{L}_{A_1,M_1} \longrightarrow \widetilde{L}_{A_2,M_2}$, defined for $A_2 \subset A_1$ and $M_2 \leq M_1$ (these homomorphisms are induced by the projection $W_{M_1}(\mathbb{F}_{q_0}) \longrightarrow W_{M_2}(\mathbb{F}_{q_0})$ and the correspondence $\widetilde{V}_0 \mapsto \widetilde{V}_0$). Clearly, $\widetilde{L} = \varprojlim_{A,M} \widetilde{L}_{A,M}$ is a profree Lie $\mathbb{Z}_p$-algebra with the set of topological generators

$$\prod_{a\in\mathbb{Z}^+(p)} \mathrm{Hom}(W(\mathbb{F}_{q_0}), W(\mathbb{F}_p))_a \oplus W(\mathbb{F}_p)\widetilde{V}_0.$$

Set $L_{A,M} = \widetilde{L}_{A,M}/C_p(\widetilde{L}_{A,M}), L = \widetilde{L}/C_p(\widetilde{L})$ and denote by $V_{a,f}$ (respectively, V_0) the images of the generator $f \in \operatorname{Hom}(W(\mathbb{F}_{q_0}), W(\mathbb{F}_p))_a, a \in \mathbb{Z}^+(p)$, respectively, $\widetilde{V_0}$) in these algebras. As earlier, for any subfield $K_1 \subset K_{sep}$ use the notation $L_{K_1} = L \otimes O(K_1)$ for extension of scalars of the Lie algebra L and introduce the natural system of free generators

$$\{V_{a,n} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\mathbb{Z}\ \} \cup \{V_0\}$$

of the Lie algebra $L_{\mathbb{F}_{q_0}}$.

Fix $\alpha \in W(\mathbb{F}_{q_0})$, such that $\operatorname{Tr}\alpha = 1$, where $\operatorname{Tr} : W(\mathbb{F}_{q_0}) \longrightarrow W(\mathbb{F}_p)$ is induced by the trace of the extension $\mathbb{F}_{q_0}$ over $\mathbb{F}_p$. It is easy to see, that $\alpha \notin (\phi - \mathrm{id})W(\mathbb{F}_{q_0})$, where ϕ is the absolute Frobenius morphism of the ring of Witt vectors $W(\mathbb{F}_{q_0})$.

For any finite subset $A \subset \mathbb{Z}^+(p)$ and an integer $M \geqslant 0$ consider the elements

$$h_{A,M} = (\sum_{a \in A} t^a V_{a,0}) \circ (\alpha V_0) \in G(L_{A,M,K_0}).$$

and elements $g_{A,M} \in G(L_{A,M,K_{sep}})$, such that

1) $\sigma g_{A,M} = g_{A,M} \circ h_{A,M}$;

2) the system of elements $\{g_{A,M}\}$ is compatible in the projective system $\{L_{A,M,K_{sep}}\}$.

The choice of a such system of elements $\{g_{A,M}\}$ defines the compatible system of epimorphisms

$$\psi^\circ_{A,M} : \Gamma_0(p) \longrightarrow G(L_{A,M}),$$

(for any $\tau \in \Gamma_0(p)$ one has $\psi^\circ_{A,M}(\tau) = \tau g_{A,M} \circ (-g_{A,M})$).

Taking

$$\psi^\circ = \varprojlim_{A,M} \psi^\circ_{A,M} : \Gamma_0(p) \longrightarrow G(L),$$

we obtain the identification

$$\bar{\psi}^\circ : \Gamma_0(p)/C_p(\Gamma_0(p)) \simeq G(L).$$

If $g = \varprojlim_{A,M} g_{A,M}$, $h = \varprojlim_{A,M} h_{A,M}$, then $\sigma g = g \circ h$ and for any $\tau \in \Gamma_0(p)$ one has:

$$\psi^0(\tau) = \tau g \circ (-g).$$

Remark.

Let $\varepsilon_p : K_0^* \longrightarrow \Gamma_0(p)/C_2(\Gamma_0(p))$ be the homomorphism appearing from the reciprocity map of local class field theory. Via Witt explicit reciprocity law, [W], one can show that

a) $\varepsilon_p(\widetilde{t_0}) = (\bar{\psi}^0)^{-1}(V_0) \bmod C_2(\Gamma_0(p))$;

b) if $E(X)$ is Artin-Hasse exponential (c.f. n.4.2.2), $a \in \mathbb{Z}^+(p), \beta \in W(\mathbb{F}_{q_0})$, then

$$\varepsilon_p(E(\beta \widetilde{t_0}^a)) = (\bar{\psi}^0)^{-1}(V_{a,f_\beta}) \bmod C_2(\Gamma_0(p)).$$

Here the homomorphism $f_\beta \in \mathrm{Hom}(W(\mathbb{F}_{q_0}), W(\mathbb{F}_p))$ is such that for any $\alpha \in W(\mathbb{F}_{q_0})$ one has $f_\beta(\alpha) = \mathrm{Tr}(\beta\alpha)$, where

$$\mathrm{Tr} : W(\mathbb{F}_{q_0}) \longrightarrow W(\mathbb{F}_p)$$

is induced by the trace of the extension $\mathbb{F}_{q_0}/\mathbb{F}_p$.

5.2. Let $\phi_0 \in \mathrm{Gal}(K_0/\mathbb{F}_p((\tilde{t_0})))$ be such that $\phi_0(\tilde{t_0}) = \tilde{t_0}$ and $\phi_0|_{\mathbb{F}_{q_0}}$ be the absolute Frobenius automorphism of the extension $\mathbb{F}_{q_0}/\mathbb{F}_p$. It is clear, that ϕ_0 generates the Galois group $\mathrm{Gal}(K_0/\mathbb{F}_p((\tilde{t_0})))$.

Denote by a_{ϕ_0} the automorphism of the Lie algebra L, given on the set of generators

$$\{V_{a,n} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\mathbb{Z}\} \cup \{V_0\}$$

of the Lie algebra $L_{\mathbb{F}_{q_0}}$ by the following conditions:

$$a_{\phi_0} : V_{a,n} \mapsto \widetilde{\exp}(\sigma^n \alpha \,\mathrm{ad}(V_0))(V_{a,n+1})$$

$$a_{\phi_0} : V_0 \mapsto V_0$$

(here $\widetilde{\exp}(X) = \sum_{0 \le n < p} X^n/n!$ is the truncated exponential).

Proposition.

a) $\phi_0(h) \underset{R}{\sim} a_{\phi_0}(h)$;

b) the correspondence $g \mapsto a_{\phi_0}(g) \circ (\alpha V_0)$ *defines an extension* $\hat{\phi}_0$ *of the automorphism* ϕ_0 *to the field* $K_{sep}^{\mathrm{Ker}\,\psi_0}$ *(which coincides with the maximal p-extension of* K_0 *having Galois group of class of nilpotency* $< p$*);*

c) The action of $\hat{\phi}_o$ *on* $\Gamma_0(p)/C_p(\Gamma_0(p))$ *by conjugation corresponds under the identification* $\bar{\psi}^0$ *to the automorphism* a_{ϕ_0} *of the Lie algebra* $L_{\mathbb{F}_{q_0}}$.

Proof.

Indeed, a) is implied by the following calculation:

$$\phi_0(h) = (\sum_{a \in \mathbb{Z}^+(p)} t^a V_{a,1}) \circ (\sigma\alpha V_0) \underset{R}{\sim} (\alpha V_0) \circ (\sum_{a \in \mathbb{Z}^+(p)} t^a V_{a,1}) =$$

$$= [(\alpha V_0) \circ (\sum_{a \in \mathbb{Z}^+(p)} t^a V_{a,1}) \circ (-\alpha V_0)] \circ (\alpha V_0) =$$

$$= (\sum_{\substack{a \in \mathbb{Z}^+(p) \\ 0 \le m < p}} t^a \frac{\alpha^m (\mathrm{ad}\, V_0)^m}{m!} V_{a,1}) \circ (\alpha V_0) =$$

$$= \sum_{\substack{a \in \mathbb{Z}^+(p) \\ 0 \leqslant m < p}} t^a \widetilde{\exp}(\alpha \,\mathrm{ad}(V_0))(V_{a,1}) \circ (\alpha V_0) = a_{\phi_0}(h).$$

(we use the identity

$$\exp(X)\exp(Y)\exp(-X) = \exp(\sum_{n \geqslant 0} \frac{1}{n!}(\mathrm{ad}\, X)^n Y)$$

in an associative $\mathbb{Q}$-algebra with generators X, Y, c.f. [B, ch.2, n.6, exerc.1]).

From this calculation it follows that

$$\phi_0(h) = (-\alpha V_0) \circ a_{\phi_0}(h) \circ (\sigma\alpha V_0).$$

Now the part b) follows from remark 1.5.2.

The part c) of our Proposition follows from remark 1.5.4.

5.3. Let $I_0 \subset \Gamma_0(p)$ be the higher ramification subgroup. Consider the restriction ψ^* of the morphism ψ° to the subgroup I_0:

$$\psi^* = \psi^\circ|_{I_0} : I_0 \longrightarrow G(L).$$

In according with the decomposition $L = \varprojlim_{A,M} L_{A,M}$ one has the decomposition $\psi^* = \varprojlim_{A,M} \psi^*_{A,M}$, where $\psi^*_{A,M}$ is a compatible system of homomorphisms

$$\psi^*_{A,M} : I_0 \longrightarrow G(L_{A,M}).$$

Proposition. *There exists $\beta \in W(k)$, such that*

1) $\sigma\beta - \beta = \alpha$;

2) if $g^*_{A,M} = g_{A,M} \circ (-\beta V_0)$ and

$$h^*_{A,M} = \sum_{a \in A} \Big(\sum_{0 \leq m < p-1} \frac{\beta^m}{m!} (\mathrm{ad})^m (V_{a,0}) \Big) t^a,$$

then $\psi^*_{A,M} = \pi_{g^*_{A,M}}(h^*_{A,M})$, i.e. (in notation of the Corollary 1.4) for any $\tau \in I_0$ it holds:

$$\psi^*_{A,M}(\tau) = \tau(g^*_{A,M}) \circ (-g^*_{A,M})$$

$$\sigma g^*_{A,M} = g^*_{A,M} \circ h^*_{A,M}.$$

Proof.

Let L° be the free commutative Lie $\mathbb{Z}_p$ -algebra with the generator V_0. For an integer $M \geqslant 0$ set $L^\circ_M = L^\circ / p^{M+1} L^\circ$. Consider the morphism of Lie $\mathbb{Z}_p$-algebras

$$\pi_{A,M} : L_{A,M} \longrightarrow L^\circ_M,$$

given in the terms of generators by the following conditions $V_{a,f} \mapsto 0$ and $V_0 \mapsto V_0$ for all $a \in A \subset \mathbb{Z}^+(p), f \in \mathrm{Hom}(W_M(\mathbb{F}_{q_0}), W_M(\mathbb{F}_p))$.

The epimorphisms $\pi_{A,M}$ define the epimorphism

$$\pi = \varprojlim_{A,M} \pi_{A,M} : L \longrightarrow L^\circ.$$

Clearly, if $L^* = \mathrm{Ker}\,\pi$, then $\mathrm{Im}\,\psi^*(I_0) = G(L^*) \subset G(L)$.

Consider the extension of scalars of the morphism π:

$$\pi_{K_{sep}} : L_{K_{sep}} \longrightarrow L^{\circ}_{K_{sep}}.$$

Then $\pi_{K_{sep}}(g) = \beta V_0$, where $\beta \in W(k)$ is such that

$$\sigma\beta - \beta = \alpha.$$

It is clear, that β generates the maximal unramified p-extension of the field K_0. Set $g = g^* \circ (\beta V_0)$ in $G(L_{K_{sep}})$. If $g^* = \varprojlim_{A,M} g^*_{A,M}$, then $g_{A,M} = g^*_{A,M} \circ (\beta V_0)$ and

$$\psi^*_{A,M}(\tau) = \psi^0_{A,M}(\tau) = \tau(g_{A,M}) \circ (-g_{A,M}) = \tau(g^*_{A,M}) \circ (-g^*_{A,M}).$$

Introduce $h_1 \in G(L_{K_0})$ by the equality

$$h = h_1 \circ (\alpha V_0).$$

The following equalities

$$\sigma g = g \circ h = g^* \circ (\beta V_0) \circ h_1 \circ (\alpha V_0),$$

$$\sigma g = \sigma g^* \circ (\sigma\beta V_0) = \sigma g^* \circ (\beta V_0) \circ (\alpha V_0)$$

give

$$\sigma g^* = g^* \circ h^*,$$

where $h^* = (\beta V_0) \circ h_1 \circ (-\beta V_0) \in G(L_K)$.

Let $h^* = \varprojlim_{A,M} h^*_{A,M}$, $h_1 = \varprojlim_{A,M} (h_1)_{A,M}$. Then

$$(h_1)_{A,M} = \sum_{a \in A} t^a V_{a,0}$$

and, therefore,

$$h^*_{A,M} = \beta V_0 \circ (\sum_{a \in A} t^a V_{a,0}) \circ (-\beta V_0) = \sum_{\substack{a \in A \\ 0 \le m < p}} \frac{\beta^m}{m!} t^a (\operatorname{ad} V_0)^m (V_{a,0})$$

Proposition is proved.

5.4. *Construction of the morphism δ.*

As was proved earlier the morphism

$$\psi^* = \psi^{\circ}|_{I_0} : I_0 \longrightarrow G(L)$$

is given by the correspondence $\tau \mapsto (\tau g^*) \circ (-g^*)$, where $\sigma g^* = g^* \circ h^*$.

On the other hand, the morphism

$$\psi(p) : \Gamma(p) \longrightarrow G(\mathcal{L}(p))$$

(c.f. n.3.5.2) is given by the correspondence

$$\tau \mapsto \tau f(p) \circ (-f(p)),$$

where $f(p) \in \mathcal{L}_{K_{sep}}$, $\sigma f(p) = f(p) \circ e$, $e(p) = \varprojlim e_{A,N,M}$ and $e_{A,N,M} = \sum_{a\in A} t^a D_{a,0}$ (as usually, $A \subset \mathbb{Z}^+(p)$ is a finite subset, $N \geqslant 1, M \geqslant 0$ are integers).

Therefore, an explicit form of the morphism $\delta : \mathcal{L}(p) \longrightarrow L$ can be obtained from the conditions

$$\delta_K(e) = h^*, \quad \delta_{K_{sep}}(f(p)) = g^*.$$

Let $\mathcal{L}_{A,N,M}$ be the Lie algebra from n. 2.3 and

$$\{ D_{a,n} \mid a \in A, n \in \mathbb{Z}/N\mathbb{Z} \}$$

be the standard basis of its extension of scalars $\mathcal{L}_{A,N,M,k}$.

Proposition. *If $N \equiv 0 \bmod(p^{M+1}N_0)$, then there exists a unique morphism of Lie $\mathbb{Z}_p$-algebras*

$$\delta_{A,N,M} : \mathcal{L}(p)_{A,N,M} \longrightarrow L_{A,M},$$

which satisfies the following condition:

$$\delta_{A,N,M,k}(D_{a,0}) = V_{a,0} + \sum_{1\leq m<p} \frac{\beta^m}{m!}(\operatorname{ad} V_0)^m(V_{a,0}) = \widetilde{\exp}(\beta \operatorname{ad}(V_0))(V_{a,0})$$

(here $\delta_{A,N,M,k} = \delta_{A,N,M} \otimes W(k)$).

Proof.

One should check up that the morphism of Lie algebras

$$\delta_{A,N,M,k} : \mathcal{L}_{A,N,M,k} \longrightarrow L_{A,M,k},$$

which is given by the relation $\delta_{A,N,M,k}(D_{a,n}) = \sigma^n \delta_{A,N,M,k}(D_{a,0})$ for $0 \leq n < N, a \in A$, commutes with the action of σ on these Lie algebras.

It is sufficient to prove that

$$\sigma^N(\delta_{A,N,M,k}(D_{a,0})) = \delta_{A,N,M,k}(D_{a,0}).$$

This fact is implied by the following lemma

Lemma.
If $N \equiv 0 \bmod(p^{M+1}N_0)$, then $\sigma^N(\beta) \equiv \beta \bmod p^{M+1}$.

Proof.

One has

$$\sigma^{N_0}\beta = \beta + \alpha + ... + \sigma^{N_0-1}\alpha = \beta + \operatorname{Tr}\alpha = \beta + 1.$$

Therefore,

$$\sigma^N\beta = \beta + \frac{N}{N_0} \equiv \beta \bmod p^{M+1}.$$

Corollary.

a)

$$\delta = \varprojlim \delta_{A,N,M}.$$

b) if $N \equiv 0 \bmod p^{M+1}N_0, a \in \mathbb{Z}^+(p), l \in \mathbb{Z}$, *then one has in the Lie algebra* $L_{A,M,k} = L_{A,M} \otimes W(k)$ *the equality*

$$\delta_{A,N,M,k}(D_{a,j_N(l)}) = \widetilde{\exp}(\sigma^l \beta\, \mathrm{ad}(V_0))(V_{a,j_{N_0}(l)})$$

(here $j_N(l)$ *and* $j_{N_0}(l)$ *are the residues of* l *modulo* N *and* N_0*, respectively).*

Proof.

From the above propositions of nn.5.3, 5.4 it follows that for $N \equiv 0 \bmod(p^{M+1}N_0)$ $\delta_{A,N,M,K}$ transforms

$$e_{A,N,M}(p) = \sum_{a \in A} t^a D_{a,0} \in G(\mathcal{L}_{A,N,M,K_{tr}})$$

to $h^*_{A,M} \in G(L_{A,M,K})$.Therefore,

$$\varprojlim \delta_{A,N,M,K} = \delta_K,$$

and we obtain the part a) of the above statement.

Using the commutativity of δ and σ we obtain the formula of the part b) of our Corollary.

5.5. Let $\{L^{(v)}\}_{v>0}$ be a filtration of the Lie algebra L, which corresponds to the ramification filtration of the Galois group $\Gamma_0(p)$ under the identification $\bar{\psi}^0$.

5.5.1. Let $\phi_0 \in \mathrm{Gal}(K_0/\mathbb{F}_p((\tilde{t_0})))$ be the automorphism from n.5.2 and $\hat{\phi}_0$ be its extension to an automorphism of the maximal p-extension of the field K_0 with Galois group of class of nilpotence $< p$ from the Proposition 5.2 c).

For any $l \in L_k = L \otimes W(k)$ set

$$\phi_0 * l = a_{\phi_0}(l),$$

where a_{ϕ_0} is the automorphism of the Lie algebra L from n.5.2. As was proved in the Proposition 5.2, the morphism $l \mapsto \phi_0 * l, l \in L_k$, gives (in the terms of Lie algebras) the action of the lifting $\hat{\phi}_0$ on the group $\Gamma_0(p)/C_p(\Gamma_0(p))$ by conjugation.

For any $m \in \mathbb{Z}$ denote by ϕ_0^m the m-th iteration of the morphism $l \mapsto \phi_0 * l$.

5.5.2. Let $v \in \mathbb{Q}, v > 0$. For any $\gamma \in \mathbb{Q}, \gamma > 0$, consider the elements $\mathcal{G}_v(\gamma) \in L_{\mathbf{F}_{q_0}}$, which are given by the following expressions:

$$\mathcal{G}_v(\gamma) =$$

$$= \sum_{\substack{1 \leqslant s < p \\ a_1,\dots,a_s \in \mathbb{Z}^+(p) \\ i,m_2,\dots,m_s \geqslant 0 \\ p^i(a_1 + \frac{a_2}{p^{m_2}} + \dots + \frac{a_s}{p^{m_s}} = \gamma \\ p^i a_1,\dots,p^i a_s < (p-s)v}} (-1)^s p^i a_1 \eta(0, m_2, \dots, m_s)[\dots[\phi_0^i * V_{a_1,0}, \phi_0^{i-m_2} * V_{a_2,0}], \dots, \phi_0^{i-m_s} * V_{a_s,0}].$$

5.5.3. Theorem. *In notation of n.5.5.2 $L^{(v)}$ is the minimal ideal of the Lie algebra L, such that $L^{(v)} \otimes W(\mathbb{F}_{q_0})$ contains the following elements:*

a) $p^i V_{a,0}$, if $p^i a \geqslant (p-1)v$;

b) $\mathcal{G}_v(\gamma)$, if $\gamma \geqslant v$.

5.6. *Proof of Theorem* 5.5.3.

5.6.1. For any $M \geqslant 0$ set $L_M = \varprojlim_A L_{A,M}$, then $L = \varprojlim_M L_M$.

Analogously, let $\mathcal{L}(p)_{N,M} = \varprojlim_A \mathcal{L}_{A,N,M}$, then $\mathcal{L}(p) = \varprojlim_{N,M} \mathcal{L}(p)_{N,M}$.

For $N \equiv 0 \bmod N_0 p^{M+1}$ consider the morphism

$$\delta_{N,M} = \varprojlim_A \delta_{A,N,M} : \mathcal{L}(p)_{N,M} \longrightarrow L_M$$

(c.f. n.5.4).

It follows from n.3.5.4, that $\mathcal{L}(p)^{(v)} = \varprojlim_{N,M} \mathcal{L}(p)^{(v)}_{N,M}$, and the ideals $\mathcal{L}(p)^{(v)}_{N,M}$ are the minimal ideals of the Lie algebra $\mathcal{L}(p)_{N,M}$ such that $\mathcal{L}(p)^{(v)}_{N,M} \otimes W(k)$ contains the elements

a) $p^i D_{a,0}$, where $a \in \mathbb{Z}^+(p), i \geqslant 0, p^i a \geqslant (p-1)v$;

b) $\mathcal{F}_{N,v}(\gamma, 0)$ for $\gamma \geqslant v$.

Therefore, $L^{(v)}_M$ is the minimal ideal of the Lie algebra L_M, such that $L^{(v)}_M \otimes W(k)$ contains the elements

a) $p^i \delta_{N,M}(D_{a,0})$, where $p^i a \geqslant (p-1)v$;

b) $\delta_{N,M}(\mathcal{F}_{N,v}(\gamma, 0))$, where $\gamma \geqslant v$.

5.6.2. As earlier, for any $l \in \mathbb{Z}$ denote by $j_N(l)$ the residue of l modulo N.

Lemma. *For any $a \in \mathbb{Z}^+(p)$ and $l \in \mathbb{Z}$ in the Lie algebra $L_{M,k}$ we have the equality:*

$$\delta_{N,M,k}(D_{a,j_N(l)}) = \widetilde{\exp}(\beta \operatorname{ad} V_0)(\phi_0^l * V_{a,0}).$$

Remark. The automorphism $l \mapsto \phi_0 * l$ of the Lie algebra $L_{M,k}$ has the order $N_0 p^{M+1}$ (c.f. the proof of the Lemma n.5.4), therefore, the element $\phi_0^l * V_{a,0}$ depends only on the residue $j_N(l)$.

Proof.

For any $l \in \mathbb{Z}$ one has (c.f. the Corollary n.5.4)

$$\delta_{N,M,k}(D_{a,j_N(l)}) = \widetilde{\exp}(\sigma^l \beta \operatorname{ad}(V_0))(V_{a,j_{N_0}(l)}).$$

Let $l \equiv l_1 \bmod N$, where $l_1 \in \mathbb{Z}, 0 \leqslant l_1 < N$. Now the statement of our Lemma follows from the following identities:

1) $\sigma^l \beta - \beta \equiv \sigma^{l_1} \beta - \beta = \alpha + \sigma\alpha + \ldots + \sigma^{l_1 - 1}\alpha \bmod p^{M+1}$;

2) $\widetilde{\exp}((\alpha + \sigma\alpha + \ldots + \sigma^{l_1-1}\alpha) \operatorname{ad}(V_0))(V_{a,j_{N_0}(l)}) =$

$$= \phi_0^{l_1} * V_{a,0} = \phi_0^l * V_{a,0}.$$

5.6.3. If $N \equiv 0 \bmod N_0 p^{M+1}, a \in \mathbb{Z}^+(p), i \in \mathbb{Z}, i \geqslant 0$, then the above Lemma gives in the Lie algebra $L_{M,k}$ the following equality

$$\delta_{N,M,k}(p^i D_{a,0}) = \widetilde{\exp}(\beta \operatorname{ad} V_0)(p^i V_{a,0}).$$

For any $l_1, l_2 \in L_{M,k}$ one has the following identity

$$\widetilde{\exp}(\beta \operatorname{ad} V_0)[l_1, l_2] = [\widetilde{\exp}(\beta \operatorname{ad} V_0) l_1, \widetilde{\exp}(\beta \operatorname{ad} V_0) l_2].$$

Therefore, for any $\gamma \in \mathbb{Q}, \gamma > 0$, in $L_{M,k}$ we have the equality

$$\delta_{N,M,k}(\mathcal{F}_{N,v}(\gamma, 0)) = \widetilde{\exp}(\beta \operatorname{ad} V_0) \mathcal{G}_v(\gamma).$$

The operator $\widetilde{\exp}(\beta \operatorname{ad} V_0)$ is inversible on $L_{M,k}$, therefore, it follows from n.5.6.1 that the ideal $L^{(v)}_{M,k} = L^{(v)}_M \otimes W(k)$ is generated by the elements

a) $p^i V_{a,0}$, for $p^i a \geqslant (p-1)v$;

b) $\mathcal{G}_v(\gamma)$, for $\gamma \geqslant v$.

Now it is sufficient to remark that these elements are in the algebra $L_M \otimes W(\mathbb{F}_{q_0})$ and do not depend on M.

Theorem is proved.

5.7. As in n.3.5, we have the following version of the Theorem 5.3.3.

Theorem. *Let $1 \leqslant s_0 < p$, $v \in \mathbb{Q}, v > 0$. Then the ideal $L^{(v)} \bmod C_{s_0+1}(L)$ is the minimal ideal of the Lie algebra $L \bmod C_{s_0+1}(L)$ such that $L^{(v)} \otimes W(\mathbb{F}_{q_0}) \bmod C_{s_0+1}(L_{\mathbb{F}_{q_0}})$ contains the following elements:*

1) $p^i V_{a,0}$, where $i \geqslant 0, a \in \mathbb{Z}^+(p), p^i a \geqslant s_0 v$;

2) $\mathcal{G}_{v,s_0}(\gamma) =$

$$= \sum_{\substack{1 \leqslant s \leqslant s_0 \\ a_1, \dots, a_s \in \mathbb{Z}^+(p) \\ i, m_2, \dots, m_s \geqslant 0 \\ p^i(a_1 + \frac{a_2}{p^{m_2}} + \dots + \frac{a_s}{p^{m_s}}) = \gamma \\ p^i a_1, \dots, p^i a_s < (s_0+1-s)v}} (-1)^s p^i a_1 \eta(0, m_2, \dots, m_s)[\dots[\phi_0^i * V_{a_1,0}, \phi_0^{i-m_2} * V_{a_2,0}], \dots, \phi_0^{i-m_s} * V_{a_s,0}],$$

where $\gamma \geq v$.

References

[A] V.A.Abrashkin, *Ramification filtration of the Galois group of a local field*, (to appear in Adv. Sov. Math.).

[B] N.Bourbaki, *Lie groups and Lie algebras*, Part I: Chapters 1-3, Hermann, 1975.

[B-M] P. Berthelot, W. Messing, *Théorie de Deudonné Cristalline III: Théorèmes d'Équivalence et de Pleine Fidélité*, The Grotendieck Festschrift (P.Cartier etc., eds.), A Collection of Articles Written in Honor of 60th Birthday of Alexander Grothendieck, vol. 1, Birkhauser, 1990.

[F] J.-M. Fontaine, *Représentations p-adiques des Corps Locaux*, The Grotendieck Festschrift (P.Cartier etc., eds.), A Collection of Articles Written in Honor of 60th Birthday of Alexander Grothendieck, vol. 2, Birkhauser, 1990.

[Sh] I.R. Shafarevich, *A general reciprocoty law*, Mat. Sb. **26 (68)** (1950), 113-146.

[Se] J.-P.Serre, *Local fields*, (Graduate texts in math.; 67). Springer-Verlag, Berlin-Heidelberg-New York. Translation of Corps Locaux, 1979.

[W] E. Witt, *Zyklische Korper und Algebren der Charakteristik p vom Grad p^n*, J.Reine Angew. Math **176** (1937), 126-140.