A ramification filtration of the Galois group of a local field

Abrashkin Victor A.

Moscow Institute of the Engineers of the Civil Aviation
Kronshtadtskiy bul.
Moscow 125493

Russia

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

MPI / 93-11

0. Introduction.

Let K be a local complete discrete valuation field with perfect residue field k of characteristic p. We denote by K_{sep} a separable closure of K and by $\Gamma = Gal(K_{sep}/K)$ the absolute Galois group of K. Consider the standard tower of algebraic extensions

$$K \subset K_{ur} \subset K_{tr} \subset K_{sep}$$

where K_{ur} (resp., K_{tr}) is a maximal unramified (resp., tamely ramified) subfield of K_{sep}. This gives us a filtration of Γ:

$$\Gamma \supset \Gamma^{(0)} \supset I,$$

where $K_{ur} = K_{sep}^{\Gamma^{(0)}}$ and $K_{tr} = K_{sep}^{I}$. It is known that the tamely ramified subquotient $\Gamma^{(0)}/I$ of Γ is a procyclic group of order relatively prime to p. I is a pro-p-group, which is a profree if $charK = p$. The group theoretic structure of Γ/I as well as the arithmetic nature of the above filtration are well known. A further decomposition of Γ is related to a decreasing filtration $\{\Gamma^{(v)}\}_{v>0}$ of normal subgroups of I. These $\Gamma^{(v)}$ are called the ramification subgroups of I in upper numbering. This filtration plays a very important rôle in many arithmetic topics:

(a) Let L be a finite Galois extension of K with Galois group $\Gamma_{L/K}$. The knowledge of the image of the filtration $\{\Gamma^{(v)}\}_{v\geq 0}$ in $\Gamma_{L/K}$ gives us full information about the values of the differente and the discriminant of L/K.

(b) Most applications of the local classfield reciprocity map $\psi : K^* \longrightarrow \Gamma^{ab}$ use the arithmetic structure of K^*. This structure is related to a filtration $\{U_n\}_{n\geq 0}$ of K^*, where $U_n = \{u \in O_K \mid u \equiv 1(\pi_K^n)\}$ (π_K is any uniformiser of the valuation ring O_K of K), which corresponds under ψ exactly to the image of $\{\Gamma^{(v)}\}_{v\geq 0}$ in Γ^{ab}.

(c) Though an explicit description of Γ in purely group theoretic terms is known, c.f. [J-W], [Jac], there is a principal difficulty in applying it somewhere. The reason is the absence of any information about the arithmetic nature of the known generators and relations. A description of the ramification filtration in terms of these generators would certainly provide us with this arithmetic information.

(d) Let $charK = 0$. There is no arithmetic in the description of finite commutative group schemes G_K over K. They are just simply representations of Γ in a module $G(K_{sep})$ and can be described in purely group theoretic terms. But the question which of these representations arise from group schemes G over a valuation ring O of K gives a lot of arithmetic. For example, the property "an abelian variety A over K has a good reduction over K"closely related to the property "group schemes $Ker(p^n id_A), n \geq 1$, can be defined over O". All known properties of Γ-modules H, which arise from a finite flat commutative group scheme over O, can be expressed in terms of the ramification filtration. They are:

(d_1) "Serre's conjecture" about the action of the tamely ramified part of Γ on a semisimple envelope of H, [Se1],[R];

(d_2) the condition for the action of $\Gamma^{(v)}$ to be trivial on H for any $v > v_0(H)$, where $v_0(H)$ depends on some invariants of K and H, [F1]. In some cases these conditions are also sufficient for H to be realised in the form $G(K_{sep})$, where G is a group scheme over O,[A1],[A2].

(e) The similar problem about representations of Γ in the étale cohomology of proper schemes over K, having a good reduction ($\equiv$ we have a lot of arithmetic) gives us the same picture, [F2],[A3],[A4].

(f) The problem of the study of the ramification filtration is interesting by itself. Some information about the nontrivial character of this filtration was obtained by E.Maus, [Ma], and Gordeev,[Go].

The main purpose of this paper is to show the possibility of giving an explicit description of the ramification filtration $\{\Gamma^{(v)}\}_{v\geqslant 0}$ in group theoretic terms. We consider the simplest case of the problem: $charK = p$, $k = \bar{\mathbf{F}}_p$. The reasons are : 1) the subgroup $I = \bigcup\limits_{v>0} \Gamma^{(v)}$ of Γ is a pro-p-free group, so we have no additional problems with the abstract group theoretic structure of I; 2) the requirement that the residue field k of K is algebraically closed does not affect the ramification filtration and gives us the possibility of identifying Γ and $\Gamma^{(0)}$; 3) the arithmetical properties of K depend on its cohomological dimension n, so we treat the case $n = 1$.

Our main result gives us an explicit description of the ramification filtration modulo subgroup $I^pC_p(I)$, where $C_p(I)$ is the subgroup of Γ generated by all commutators having length p. We now outline the basic steps of our approach.

The first thing we need is some generalisation of the Artin-Schreier theory.

Let K now be an arbitrary field of characteristic p. Classical Artin-Schreier theory gives an explicit description of any p-elementary extension of K with an action of the Galois group. E.Witt gave an extension of this theory to the case of cyclic extensions, [Wtt]. A matrix form of this theory was developped by H.Inaba, [In1-3]. Under this approach it is possible to treat arbitrary extensions of K, but as a matter of fact it gives us a theory of representations of Γ in vector spaces over $\mathbf{F}_p$. The invariant form of this theory appeared in the study of crystalline representations, [F3],[A3] (from this point of view the solution of Grothendieck's problem of "mysterious "functor can be considered as the high point of the Artin-Schreier theory, [F-M],[Fa]). But this generalisation is not very convenient if we want to study the Galois group itself (rather than its image under some modular representation).

We construct our version of the Artin-Schreier theory in n.1. Our construction depends on the choise of some filtered associative bialgebra (f.a.b.) over $\mathbf{F}_p$ (c.f. 1.1.1) and its area of applicability depends on some condition (C_{s_0}), c.f. 1.1. We construct such f.a.b. objects, which satisfy the condition (C_{s_0}) for any $s_0 < p$, and apply this construction to the study of extensions of K with the Galois group of exponent p and class of nilpotency $< p$. In this case the Galois group of such extensions may be related in a very natural way to some Lie algebra over $\mathbf{F}_p$ (having class of nilpotency $< p$) and in these terms the action of the Galois group can be described explicitly, c.f. n.2.

We specify our arguments in n.3 in the case of a local complete discrete valuation field K of characteristic p. So, we have an explicit description of the extension $\widetilde{K} = K_{sep}^{I^pC_p(I)}$ over K (here $C_p(I)$ is the subgroup of the higher ramification subgroup I generated by all commutators of order $\geq p$) in terms of a profree Lie $\mathbb{F}_p$-algebra $\mathcal{L}$. Under some identification, the Galois group $Gal(\widetilde{K}/K_{tr})$ and the Lie algebra $\widetilde{\mathcal{L}} = \mathcal{L}/C_p(\mathcal{L})$ (where $C_p(\mathcal{L})$ is the ideal of $\mathcal{L}$ generated by all commutators of length

$\geq p$) are related by the truncated exponent.

In n.4 we define a decreasing filtration $\{\widetilde{\mathcal{L}}^{(v)}\}_{v>0}$ of $\widetilde{\mathcal{L}}$ by its ideals $\widetilde{\mathcal{L}}^{(v)}$, $v>0$. The description of this filtration becomes more clear when considered over $k=\bar{\mathbf{F}}_p$ (c.f. n.5).

The main theorem (c.f. n.7) shows that if the residue field of K is $k=\bar{\mathbf{F}}_p$ then the truncated exponent transfers the above filtration $\{\widetilde{\mathcal{L}}^{(v)}\}_{v>0}$ to the image of the ramification filtration $\{\Gamma^{(v)}\}_{v>0}$ of the Galois group $\Gamma = Gal(K_{sep}/K)$ in $Gal(\widetilde{K}/K)$.

It is almost clear now that this aproach must work without "mod $I^pC_p(I)$" and "$charK=p$" assumptions. We can apply the characteristic p version of the Campbell-Hausdorff formula for the construction of an f.a.b. objects, satisfying the condition (C_{s_0}) for $s_0>p$, [Di]. The Fontaine-Wintenberger functor "les corps norms ", [Wnt], works very well in extending our description to the characteristic zero case. But the general picture is not clear now so we put off the discussion on this subject till a following paper.

The main results of this paper were obtained by author during his staying in Uthrecht University (Holland, Febr.91-May 91) and in the Max Planck Institut für Mathematik (Bonn, Febr.92-Jan.93). I would like to express my gratitude to these organisations (and especially to the organisers of these visits: Prof. G.van der Geer, Prof. F.Oort and Prof. F.Hirzebruch) for their hospitality.

1. One generalisation of the Artin-Schreier theory.

1.1. The statement of the main theorem.

Let k be any field.

1.1.1.Definition.

A is a filtered associative bialgebra (f.a.b.) over k, if

a) A is an associative k-algebra with the unit element $1_A=1$;

b) there is a decreasing filtration in A:

$$A=J_0(A)\supset J_1(A)\supset ...\supset J_n(A)\supset ...,$$

where all $J_n(A)$ are two sided ideals, $J_{n_1}(A)J_{n_2}(A)\subset J_{n_1+n_2}(A)$ for all $n_1,n_2\geq 0$ and $A=k1_A\oplus J_1(A)$ as a k-module;

c) there is the structure of a coassociative coalgebra over k on A, which is given by the $k-$algebra morphisms: $\Delta : A\longrightarrow A\otimes A$ (comultiplication) and $\varepsilon : A\longrightarrow k$ (counit);

d) for every $n\geq 1$ we have $\Delta(J_n(A))\subset \underset{n_1+n_2=n}{\oplus} J_{n_1}(A)\otimes J_{n_2}(A)$ and $\varepsilon(J_n(A))=0$.

If A,B are f.a.b. over k then $A\otimes_k B$ is equipped with the natural structure of an f.a.b. over k. We note that for $n\geq 0$, $J_n(A\otimes B)=\sum\limits_{n=n_1+n_2} J_{n_1}(A)\otimes J_{n_2}(B)$.

If K is any extension of k and A is an f.a.b. over k then $A\otimes_k K$ has the natural structure of an f.a.b. over K.

1.1.2. Let A be any f.a.b. over k and s any nonnegative integer.

Definition. $a \in A/J_{s+1}(A)$ is called s-diagonal if for some (and hence for any) $\hat{a} \in A$ such that $a = \hat{a} \bmod J_{s+1}(A)$ we have: $\Delta(\hat{a}) \equiv \hat{a} \otimes \hat{a} \bmod J_{s+1}(A \otimes A)$ and $\varepsilon(\hat{a}) = 1$.

We shall denote the set of all s-diagonal elements in A by $G_A(s)$. Obviously, $G_A(s)$ is a group with respect to the operation induced by the multiplication in A. For $s_1 \geq s_2$ the quotient morphisms $A/J_{s_1+1}(A) \longrightarrow A/J_{s_2+1}(A)$ induce the reduction morphisms $r_{s_1,s_2} : G_A(s_1) \longrightarrow G_A(s_2)$.

Definition. An f.a.b. A defined over $\mathbf{F}_p$ satisfies the condition (C_{s_0}), if for all natural numbers s_1, s_2, such that $s_2 \leq s_1 \leq s_0$, and all fields K, the map

$$r_{s_1,s_2} : G_{A_K}(s_1) \longrightarrow G_{A_K}(s_2)$$

is an epimorphism.

1.1.3. Let A be an f.a.b. over the field K, L any Galois extension of K and $Gal(L/K)$ its Galois group. For any natural number consider the groups $G_A(s)$ and $G_{A_L}(s)$ of s-diagonal elements in A and $A_L = A \otimes L$, respectively. Obviously,

$$\{a \in G_{A_L}(s) |\ \tau a = a \quad \text{for all } \ \tau \in Gal(L/K)\} = G_A(s).$$

1.1.4. Let p be any prime, let A be an f.a.b. over $\mathbb{F}_p$ and let K be any field of characteristic p. For $s \geq 1$ we use the notation $G_{\mathbb{F}_p}(s)$ and $G_K(s)$ for the groups of s-diagonal elements in A and $A \otimes K$, respectively. The absolute Frobenius morphism of K acts on $G_K(s)$ and we shall use the notation $a^{(p)}$ for the image of $a \in G_K(s)$ under this action.

We have

$$\{a \in G_K(s) \mid a = a^{(p)}\} = G_{\mathbb{F}_p}(s).$$

We introduce an equivalence relation R_s on $G_K(s)$:

for any $a_1, a_2 \in G_K(s)$, $a_1 \equiv a_2 \mod R_s$ *iff there exists* $b \in G_K(s)$ *such that* $a_1 = b^{-1} a_2 b^{(p)}$.

Let K_{sep} be a separable closure of K, $\Gamma = Gal(K_{sep}/K)$. By the definition:

$f_1, f_2 \in Hom(\Gamma, G_{\mathbb{F}_p}(s))$ are in the same conjugation class iff there exists $c \in G_{\mathbb{F}_p}(s)$ such that $f_1(\tau) = c^{-1} f_2(\tau) c$ for any $\tau \in \Gamma$.

Theorem. *Let K be a field of characteristic $p > 0$ and A be an f.a.b. over $\mathbb{F}_p$ satisfying for some $s_0 \geq 1$ the condition (C_{s_0}). Then for any $s \leq s_0$ there exists a one-to-one correspondence*

$$\tilde{\pi}_s : \{G_K(s)/R_s\} \longrightarrow \{ \text{ conj. cl. of } Hom(\Gamma, G_{\mathbb{F}_p}(s))\}$$

Remark. It follows from the proof below, that these correspondences agree on s, i.e. for any $s_2 \leq s_1 \leq s_0$ the following diagramm is commutative:

$$\begin{array}{ccc}
\{G_K(s_1)/R_{s_1}\} & \xrightarrow{\tilde{\pi}_{s_1}} & \{ \text{ conj. cl. } Hom(\Gamma, G_{\mathbb{F}_p}(s_1))\} \\
{\scriptstyle r_{s_1,s_2}}\downarrow & & \downarrow{\scriptstyle r_{s_1,s_2 *}} \\
\{G_K(s_2)/R_{s_2}\} & \xrightarrow{\tilde{\pi}_{s_2}} & \{ \text{ conj. cl. } Hom(\Gamma, G_{\mathbb{F}_p}(s_2))\}
\end{array}$$

1.2.

Proof of theorem. Let L be any algebraic extension of K and $e \in G_K(s)$ for some $s \geq 0$. Consider the set

$$M_s(L,e) = \{f \in A_L/J_{s+1}(A_L) | f \in G_L(s), f^{(p)} = fe\}$$

(here the f.a.b. $A_L = A \otimes L$ is obtained from A by extension of scalars).

1.2.1. Lemma. *For any $s \leq s_0$ and $e \in G_K(s)$ there exists a separable extension L of K such that $M_s(L,e) \neq \emptyset$.*

Proof. For any $a \in A$ we can define its degree $d(a) = min\{n \mid a \in J_n(A)\}$. Choose a family $\{c_\alpha\}_{\alpha \in I} \subset J_1(A)$ such that for any natural number s

$$\{c_\alpha \mid \alpha \in I, c_\alpha \in J_s(A)\}$$

is an $\mathbb{F}_p$-basis of $J_s(A)$. This means also that for any $s \geq 0$ the elements of the set $\{c_\alpha \mid \alpha \in I, c_\alpha \notin J_{s+1}(A)\} \cup \{1\}$ taken $\mod J_{s+1}(A)$ give an $\mathbf{F}_p$-basis of $A/J_{s+1}(A)$.

Now we are able to choose (uniquely) $E \in A$ such that $e = E \mod J_{s+1}(A)$ and $E = 1 + \sum\limits_\alpha \eta(\alpha)c_\alpha$, where each $\eta(\alpha) \in K$ and $\eta(\alpha) = 0$ for $d(c_\alpha) > s$. We must prove that there exists $F = 1 + \sum\limits_\alpha T(\alpha)c_\alpha \in A_{K_{sep}}$ such that

(1) $F^p \equiv FE \mod J_{s+1}(A_{K_{sep}})$;
(2) $\Delta F \equiv F \otimes F \mod J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}})$.

It is clear that we can assume that $s \geq 1$ and that all $T(\alpha)$ are defined for $d(c_\alpha) < s$, in such a manner that the equivalences (1) and (2) are valid modulo $J_s(A_{K_{sep}})$ and $J_s(A_{K_{sep}} \otimes A_{K_{sep}})$, respectively.

Let

$$L_1 = K(\{T(\alpha) | d(c_\alpha) < s\}).$$

By inductive assumption $L_1 \subset K_{sep}$. It follows from part b) of the definition of f.a.b. that for any $\alpha_1, \alpha_2 \in I$

$$c_{\alpha_1}c_{\alpha_2} = \sum_{\alpha \in I} A(\alpha_1, \alpha_2; \alpha)c_\alpha,$$

where $A(\alpha_1, \alpha_2; \alpha) \in \mathbb{F}_p$ and $A(\alpha_1, \alpha_2; \alpha) = 0$ for $d(\alpha_1) + d(\alpha_2) > d(\alpha)$.

If $\alpha \in I$ and $d(c_\alpha) = s$, then the expression

$$\sum_{\alpha_1, \alpha_2 \in I} T(\alpha_1)A(\alpha_1, \alpha_2; \alpha)\eta(\alpha_2)$$

is well defined and gives an element of L_1. Indeed, if $A(\alpha_1, \alpha_2; \alpha)\eta(\alpha_2) \neq 0$ then $d(c_{\alpha_1}) + d(c_{\alpha_2}) \leq d(c_\alpha) = s$, so $d(c_{\alpha_1}) < s$ and $T(\alpha_1)$ defines an element of L_1 by the inductive assumption.

For $\alpha \in I$, such that $d(c_\alpha) = s$, we consider the extension

$$L = L_1(\{T(\alpha) | d(c_\alpha) = s\}),$$

where

$$T(\alpha)^p - T(\alpha) = \sum_{\alpha_1,\alpha_2\in I} T(\alpha_1)A(\alpha_1,\alpha_2;\alpha)\eta(\alpha_2) + \eta(\alpha).$$

Obviously, L is separable over L_1 and we can assume that $L \subset K_{sep}$. Let

$$F_1 = 1 + \sum_{d(c_\alpha)\leq s} T(\alpha)c_\alpha \in A_L.$$

By the choice of $T(\alpha)$ for $d(c_\alpha) = s$ we have $F_1^{(p)} \equiv F_1 E \operatorname{mod} J_{s+1}(A_L)$. By the inductive assumption

$$\Delta F_1 \equiv C_0(F_1 \otimes F_1) \operatorname{mod} J_{s+1}(A_L \otimes A_L),$$

where

$$C_0 = 1 + \sum_{\alpha_1,\alpha_2} \gamma(\alpha_1,\alpha_2)c_{\alpha_1} \otimes c_{\alpha_2},$$

$\gamma(\alpha_1,\alpha_2) \in L$ and $\gamma(\alpha_1,\alpha_2) = 0$ for $d(c_{\alpha_1}) + d(c_{\alpha_2}) \neq s$.

From the equivalences

$$\Delta F_1^{(p)} \equiv C_0^{(p)}(F_1^{(p)} \otimes F_1^{(p)}) \equiv C_0^{(p)}(F_1 \otimes F_1)(E \otimes E) \operatorname{mod} J_{s+1}(A_L \otimes A_L),$$

$$\Delta F_1^{(p)} \equiv \Delta F_1 \Delta E \equiv C_0(F_1 \otimes F_1)(E \otimes E) \operatorname{mod} J_{s+1}(A_L \otimes A_L),$$

it follows, that $C_0 = C_0^{(p)}$, i.e. all $\gamma(\alpha_1,\alpha_2) \in \mathbb{F}_p$.

Let us prove the existence of $C \in A$ such that $C \equiv 1 \operatorname{mod} J_s(A)$ and $\Delta C \equiv C_0(C \otimes C) \operatorname{mod} J_{s+1}(A \otimes A)$. Let

$$C = 1 + \sum_{d(c_\alpha)=s} \mu(\alpha)c_\alpha,$$

where $\mu(\alpha) \in \mathbb{F}_p$. We can assume, that

$$\Delta c_\alpha = c_\alpha \otimes 1 + 1 \otimes c_\alpha + \sum_{\alpha_1,\alpha_2\in I} B(\alpha;\alpha_1,\alpha_2)c_{\alpha_1} \otimes c_{\alpha_2}$$

for some $B(\alpha;\alpha_1,\alpha_2) \in \mathbb{F}_p$. We have $B(\alpha;\alpha_1,\alpha_2) = 0$ for $d(c_{\alpha_1}) + d(c_{\alpha_2}) < s$ from part d) of the definition of f.a.b. It is clear that the existence of C is equivalent to the existence of $\mu(\alpha) \in \mathbb{F}_p$, for all $\alpha \in I$ such that $d(c_\alpha) = s$, satisfying the following equations

$$(*) \qquad \sum_\alpha B(\alpha;\alpha_1,\alpha_2)\mu(\alpha) = \gamma(\alpha_1,\alpha_2),$$

where $\alpha_1,\alpha_2 \in I$ and $d(c_{\alpha_1}) + d(c_{\alpha_2}) = s$.

The coefficients and free members of this system are in $\mathbb{F}_p$, so it is sufficient to prove the solvability of the system (*) in some field of characteristic p.

By the condition (C_{s_0}), $G_L(s) \longrightarrow G_L(s-1)$ is an epimorphism, therefore there exists $F_2 \in A_L$ such that $F_2 \bmod J_{s+1}(A_L) \in G_L(s)$ and $F_2 \equiv F_1 \bmod J_s(A_L)$. Let $\tilde{C} = F_1 F_2^{-1}$ then $\tilde{C} \in A_L$, $\tilde{C} \equiv 1 \bmod J_s(A_L)$ and

$$\Delta\tilde{C} \equiv (\Delta F_1)(\Delta F_2)^{-1} \equiv C_0(F_1 \otimes F_1)(F_2 \otimes F_2)^{-1} \equiv C_0(\tilde{C} \otimes \tilde{C}) \bmod J_{s+1}(A_L \otimes A_L).$$

If

$$\tilde{C} \equiv 1 + \sum_{d(c_\alpha)=s} \tilde{\mu}(\alpha) c_\alpha \bmod J_{s+1}(A_L),$$

then the equivalence above means that the collection $\{\tilde{\mu}(\alpha) | d(c_\alpha) = s\}$ gives the solution of the system (*) in L. So the system (*) is solvable in $\mathbf{F}_p$ and the needed element C exists.

Now for $F = C^{-1}F_1 \in A_L$ we have

$$F^{(p)} = C^{(p)-1}F_1^{(p)} \equiv C^{-1}F_1 E \equiv FE \bmod J_{s+1}(A_L),$$

$$\Delta F \equiv (\Delta C)^{-1}\Delta F_1 \equiv C_0^{-1}(C \otimes C)^{-1} C_0 (F_1 \otimes F_1) \equiv F \otimes F \bmod J_{s+1}(A_L).$$

The Lemma is proved.

1.2.2. Proposition. *Let $e \in G_K(s)$ and L be an extension of K such that $M_s(L,e) \neq \emptyset$. If $f_1, f_2 \in M_s(L,e)$, then $f_1 f_2^{-1} \in G_{\mathbf{F}_p}(s)$.*

Proof. $f_1^{(p)} = f_1 e$, $f_2^{(p)} = f_2 e$, therefore $(f_1 f_2^{-1})^{(p)} = f_1 f_2^{-1}$, i.e. $f_1 f_2^{-1} \in G_{\mathbf{F}_p}(s)$.

1.2.3. Corrolary. *Let us fix some separable closure K_{sep} of K. Then for $s \leq s_0$, $e \in G_K(s)$, there exists a uniquely determined Galois extension $K_s(e) \subset K_{sep}$ of K such that*

1. *$M_s(K_s(e), e) \neq \emptyset$;*
2. *if $M_s(L,e) \neq \emptyset$ for some subfield $L \subset K_{sep}$, then $L \supset K_s(e)$ and $M_s(L,e) = M_s(K_s(e), e)$.*

Proof. Let $L_0 \subset K_{sep}$ be some minimal element in the partially ordered (by inclusion) set of the subfields L in K_{sep} such that $M_s(L,e) \neq \emptyset$. Choose some $f_0 \in M_s(L_0, e)$.

If $L \subset K_{sep}$ is such that $M_s(L,e) \neq \emptyset$ and $f \in M_s(L,e)$ then $f_0, f_1 \in M_s(LL_0, e)$. It follows from the above proposition that $f_0, f_1 \in M_s(L \cap L_0, e)$. L_0 is minimal, so $L \cap L_0 = L_0$, i.e. $L \supset L_0$. Analogously, L_0 is the Galois extension of K. So we can take $K_s(e) = L_0$, q.e.d.

1.2.4. Now we are able to use the new notation $M_s(e)$ for the set $M_s(K_s(e), e)$.

Proposition. *Let $s_2 \leq s_1 \leq s_0$, $e_1 \in G_K(s_1), e_2 \in G_K(s_2)$ and $r_{s_1,s_2}(e_1) = e_2$, where $r_{s_1,s_2} : G_K(s_1) \longrightarrow G_K(s_2)$ is the reduction morphism from n.1.2. Then $K_{s_1}(e_1) \supset K_{s_2}(e_2)$ and r_{s_1,s_2} induces an epimorphic mapping $M_{s_1}(e_1) \longrightarrow M_{s_2}(e_2)$.*

The proof follows immediately from n.2.2.

1.2.5. Let $s \leq s_0$, $e \in G_K(s)$, $f \in M_s(e)$. For any $\tau \in \Gamma = Gal(K_{sep}/K)$ $\tau f = c(\tau) f$, where $c(\tau) \in G_{\mathbf{F}_p}(s)$. Obviously, $\tau \mapsto c(\tau)$ defines an element of $Hom(\Gamma, G_{\mathbf{F}_p}(s))$, which we denote by $\pi_{e,f,s}$. The following proposition follows immediately from the definitions.

Proposition.

(1) $Ker(\pi_{e,f,s}) = Gal(K_{sep}/K_s(e))$;

(2) *if* $f_1, f_2 \in M_s(e)$ *then* $\pi_{e,f_1,s}$ and $\pi_{e,f_2,s}$ *are conjugate under some inner automorphism of the group* $G_{\mathbb{F}_p}(s)$;

(3) *if some homomorphism* $\pi : \Gamma \longrightarrow G_{\mathbb{F}_p}(s)$ *is conjugate to* $\pi_{e,f,s}$ *then there exists* $f' \in M_s(e)$ *such that* $\pi_{e,f',s} = \pi$.

1.2.6. So, for $1 \le s \le s_0$, the correspondence $e \mapsto \{\text{conj.cl.}Hom(\Gamma, G_{\mathbb{F}_p}(s))\}$ gives the mappings

$$\tilde{\pi}_s : G_K(s) \longrightarrow \{\text{ conj. cl. } Hom(\Gamma, G_{\mathbb{F}_p}(s))\}.$$

Proposition. *Let* $e_1, e_2 \in G_K(s)$, $s \le s_0$. *Then we have:*
$\tilde{\pi}_s(e_1) = \tilde{\pi}_s(e_2) \Leftrightarrow e_1 \equiv e_2 \mod R_s$, *i.e. there exists some* $h \in G_K(s)$, *such that* $e_2 = h^{-1}e_1h^{(p)}$.

Proof. Let $f_1 \in M_s(e_1), f_2 \in M_s(e_2)$. We have:
$\tilde{\pi}_s(e_1) = \tilde{\pi}_s(e_2) \Leftrightarrow$ there exists $a \in G_{\mathbb{F}_p}(s)$ such that for any $\tau \in \Gamma$, $c_1(\tau) = a^{-1}c_2(\tau)a$, where $\tau f_1 = c_1(\tau)f_1, \tau f_2 = c_2(\tau)f_2$.

Let $h = f_1^{-1}a^{-1}f_2 \in G_{K_{sep}}(s)$. Then $h^{(p)} = f_1^{(p)-1}a^{-1}f_2^{(p)} = e_1^{-1}f_1^{-1}a^{-1}f_2e_2 = e_1^{-1}he_2$, i.e. $e_2 = h^{-1}e_1h^{(p)}$. But for any $\tau \in \Gamma : \tau h = (\tau f_1)^{-1}a^{-1}(\tau f_2) = f_1^{-1}c_1(\tau)^{-1}a^{-1}c_2(\tau)f_2 = f_1^{-1}a^{-1}f_2 = h$, i.e. $h \in G_K(s)$.

1.2.7. It follows from the previous proposition that $\tilde{\pi}_s$ defines an injective mapping

$$\pi_s : G_K(s)/R_s \longrightarrow \{\text{ conj. cl. } Hom(\Gamma, G_{\mathbb{F}_p}(s))\}.$$

The surjectivity of π_s follows from the next proposition.

Proposition. *Let* $s \le s_0$ *and* $\pi \in Hom(\Gamma, G_{\mathbb{F}_p}(s))$. *Then there exist* $e \in G_K(s)$ *and* $f \in M_s(e)$, *such that* $\pi = \pi_{e,f,s}$.

Proof. We can assume that $s > 1$ and use the induction on s. Then there exist $e_1 \in G_K(s-1)$, $f_1 \in M_{s-1}(e_1)$ such that for any $\tau \in \Gamma$, $\tau f_1 = \pi'(\tau)f_1$, where $\pi'(\tau) = \pi(\tau) \mod J_s(A)$. Choose $e_2 \in G_K(s)$ such that $r_{s,s-1}(e_2) = e_1$ and choose $f_2 \in M_s(e_2)$ such that $r_{s,s-1}(f_2) = f_1$.

Now we shall use the special $\mathbb{F}_p$-basis $\{c_\alpha\}_{\alpha \in I}$ from the proof of lemma 1.2.1. By means of this basis we can take liftings

$$E_2 = 1 + \sum_{\alpha \in I} \eta(\alpha)c_\alpha \in A_K$$

and

$$F_2 = 1 + \sum_{\alpha \in I} \mu(\alpha)c_\alpha \in A_{K_{sep}}$$

of e_2 and f_2, which are uniquely determined by the conditions $\eta(\alpha) = 0, \mu(\alpha) = 0$ if $d(c_\alpha) > s$. We have:

$$F_2^{(p)} \equiv F_2E_2 \mod J_{s+1}(A_{K_{sep}}),$$

$$\Delta F_2 \equiv F_2 \otimes F_2 \operatorname{mod} J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}}),$$

$$\tau F_2 \equiv \pi_1(\tau) F_2 \operatorname{mod} J_{s+1}(A_{K_{sep}}),$$

where $\tau \in \Gamma, \pi_1 \in Hom(\Gamma, G_{\mathbb{F}_p}(s))$ and $\pi_1 \equiv \pi \operatorname{mod} J_s(A)$.

Let $\pi_1(\tau) = c(\tau)\pi(\tau)$ for any $\tau \in \Gamma$. Then $c(\tau) \in G_{\mathbb{F}_p}(s), r_{s,s-1}(c(\tau)) = 1$ and $c(\tau_1\tau_2) = c(\tau_1)c(\tau_2)$ for any $\tau_1, \tau_2 \in \Gamma$. Let $C(\tau) \in 1 + J_s(A) \subset A$ be liftings of $c(\tau)$ of the type above. By a cohomological triviality of the Galois module K_{sep}, there exists $C_1 \in A_{K_{sep}}$, such that $C_1 \equiv 1 \operatorname{mod} J_s(A_{K_{sep}})$ and $\tau C_1 \equiv C(\tau) C_1 \operatorname{mod} J_{s+1}(A_{K_{sep}})$.

Now we have for $F_3 = C_1 F_2$:

$$\tau F_3 \equiv \pi(\tau) F_3 \operatorname{mod} J_{s+1}(A_{K_{sep}}),$$

$$\Delta F_3 \equiv (F_3 \otimes F_3) C_2 \operatorname{mod} J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}}),$$

where $C_2 \equiv 1 \operatorname{mod} J_s(A_{K_{sep}} \otimes A_{K_{sep}})$ and

$$\Delta C_1 \equiv (C_1 \otimes C_1) C_2 \operatorname{mod} J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}}).$$

For every $\tau \in \Gamma$, $(\tau C_1) C_1^{-1} \operatorname{mod} J_{s+1}(A_{K_{sep}})$ is an s-diagonal element, therefore, $\tau C_2 = C_2$, i.e. $C_2 \in (A \otimes A) \operatorname{mod} J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}})$. Similarly, as in the prove of lemma 2.1, we can obtain the existence of $C_3 \in A$ such that $C_3 \equiv 1 \operatorname{mod} J_s(A)$ and $\Delta C_3 \equiv (C_3 \otimes C_3) C_2 \operatorname{mod} J_{s+1}(A \otimes A)$. So, for $F = C_3^{-1} F_3$ we have:

$$\tau F \equiv \pi(\tau) F \operatorname{mod} J_{s+1}(A_{K_{sep}}),$$

$$\Delta F \equiv F \otimes F \operatorname{mod} J_{s+1}(A_{K_{sep}} \otimes A_{K_{sep}}).$$

It now follows, that $E = F^{(p)} F^{-1} \operatorname{mod} J_{s+1}(A_{K_{sep}})$ is the Γ-invariant element of $G_{K_{sep}}(s)$, hence $E \operatorname{mod} J_{s+1}(A_{K_{sep}}) = e \in G_K(s)$. If we set $f = F \operatorname{mod} J_{s+1}(A_{K_{sep}})$, then $\pi = \pi_{e,f,s}$.

So, the proposition and the theorem of n.2 are proved.

1.3. Examples and applications.

1.3.1. Theorem n.2 means nothing in the case $s = 0$ because for every f.a.b. A over $\mathbb{F}_p$ we have $G_{\mathbb{F}_p}(0) = G_K(0) = 1$.

Consider the first nontrivial case where our theorem works. Let $A = \mathbb{F}_p[D]$ where D is an indeterminate, with a filtration by the ideals $J_s(A) = (D^s), s \geq 0$, and coalgebra structure given by $\Delta D = D \otimes 1 + 1 \otimes D, \varepsilon(D) = 0$. It is easy to verify that for $s = 1$ and this choice of f.a.b. our theorem gives us the usual Artin-Schreier theory. Indeed we have the identifications $G_{\mathbb{F}_p}(s) = \mathbb{F}_p$, $G_K(1) = K$ given by correspondences $1 + aD \mod (D^2) \mapsto a$, where $a \in \mathbb{F}_p$ or $a \in K$. The equivalence relation R_1 on $G_K(1)$ is transformed here to the relation R on K:

$$a_1 \equiv a_2 \operatorname{mod} R \quad \text{iff } a_1 = a_2 + b^p - b \quad \text{for some } b \in K.$$

So π_1 can be considered as a one-to-one correspondence

$$\pi_1' : K/R \longrightarrow Hom(\Gamma, \mathbb{F}_p),$$

where $\Gamma = Gal(K_{sep}/K)$. It follows from the construction of π_1 that for any $a \in K$ the homomorphism $\chi = \pi_1'(a \bmod R)$ maps any $\tau \in \Gamma$ to $\chi(\tau) = \tau T - T \in \mathbf{F}_p$ where $T^p - T = a$. Of course, π_1' is also an isomorphism of groups.

Let us take any $1 \leq s < p$. It is easy to show that for these s

$$G_K(s) = \{ \widetilde{exp}(aD) \bmod J_s(A) \mid a \in K\},$$

where $\widetilde{exp}(l) = \sum\limits_{0 \leq n < p} l^n/n!$ is the truncated exponent. It means that the reduction maps $r_{s_1,s_2} : G_K(s_1) \longrightarrow G_K(s_2)$, for $1 \leq s_2 \leq s_1 < p$, are one-to-one mappings and therefore the f.a.b. A satisfies the condition (C_{p-1}). But this means also that theorem n.2 for the f.a.b. A and arbitrary $1 \leq s < p$ gives nothing more than the Artin-Schreier theory.

It may be shown that

$$G_K(p) = \{\widetilde{exp}(aD^p) \bmod J_{p+1}(A) \mid a \in K\}.$$

Therefore, $r_{p,1} : G_K(p) \longrightarrow G_K(1)$ is the zero mapping, so the f.a.b. A does not satisfy the condition (C_p).

1.3.2. Let $W = SpecB$ be the scheme of Witt vectors. We can assume that $B = \mathbf{Z}_p[Y_0, Y_1, ..., Y_n, ...]$ and the operations on W are given by means of the Witt polynomials: $w_n(Y_0, ..., Y_n) = Y_0^{p^n} + pY_1^{p^{n-1}} + ... + p^n Y_n$, $n \geq 0$.

Let $\widetilde{W} = W \otimes \mathbf{F}_p$ be the reduction of W modulo p. We have $\widetilde{W} = SpecA$, where $A = \mathbf{F}_p[X_0, X_1, ..., X_n, ...]$ and $X_n = Y_n \otimes 1$ for $n \geq 0$. The bialgebra structure on A is induced by the bialgebra structure on B. Introduce the grading of A by the conditions $d(X_n) = p^n$ for $n \geq 0$. Then the ideals

$$J_s(A) = \{a \in A | d(a) \geq s\}$$

for $s \geq 0$ define a decreasing filtration of A. So we have the structure of an f.a.b. on A.

Let $E \in \mathbf{Z}_p[[Y]]$ be the power series equal to

$$exp(Y + Y^p/p + ... + Y^{p^n}/p^n + ...)$$

(the Artin-Hasse exponent). We can consider the collection of variables

$$\bar{X} = (X_0, X_1, ..., X_n, ...)$$

as the element of the ring $\widetilde{W}(A)$ and define

$$\bar{E}(\bar{X}) = \prod_{n \geq 0} E(X_n).$$

$\bar{E}(\bar{X})$ is the element of a completion of A in the topology induced by the grading d. If K is a field of characteristic p then the collection of the coordinates of the product of Witt vectors $\bar{w}$ and $\bar{X}$ will be denoted by $\bar{w}\bar{X}$.

Proposition. *Let s be a natural number, $G_{A,K}(s)$ be the group of s-diagonal elements of the f.a.b. $A_K = A \otimes K$. Then*

$$G_{A,K}(s) = \{\bar{E}(\bar{w}\bar{X}) \bmod J_{s+1}(A_K) \mid \bar{w} \in \widetilde{W}(K)\}.$$

Proof. We remark, that elements of the $\mathbf{F}_p$-module

$$M_s = \{m \in K[X_0, ..., X_n, ...] \mid d(m) \le s\}$$

give the full set of representatives of the elements of a $A_K/J_{s+1}(A_K)$ in A_K. Let $e \in A_K/J_{s+1}(A_K)$ and $E = \sum_{i=0}^{s} E_i \in M_s$ be its representative, where E_i for $0 \le i \le s$ are isobaric polynomials of $X_0, X_1, ..., X_n, ...$ of the weight $d = i$. The coaddition Δ in A is given by the isobaric polynomials, therefore: $e \in G_{A,K}(s)$ iff $E_0 = 1$ and $\Delta E_i = \sum_{i_1+i_2=i} E_{i_1} \otimes E_{i_2}$ for $0 \le i \le s$. This means that $\sum_{0 \le i \le s} E_i t^i$ is a "curve" for $\widetilde{W}$ modulo $deg(s+1)$, c.f.[Di]. Now our proposition follows from the explicit description of all curves for the scheme of Witt vectors, [Di],n.7.

Corollary. *The f.a.b. A satisfies the condition (C_{s_0}) for any natural number s_0.*

Corollary. *For any field K of characteristic p and any natural number s, the correspondence $\bar{E}(\bar{w}\bar{X}) \mapsto \bar{w}$ gives an isomorphism*

$$G_{A,K}(s) \longrightarrow \widetilde{W}_s(K),$$

where $\widetilde{W}_s$ is the group scheme of Witt vectors of finite length s over $\mathbb{F}_p$.

So this choice of f.a.b. A gives the following result of Witt, [Wt]:

If $s \ge 1$ and K is a field of characteristic $p > 0$ then there exists a one-to-one correspondence

$$W_s(K)/(F - id)W_s(K) \longrightarrow Hom(\Gamma, \mathbf{Z}/p^s\mathbf{Z})$$

(here $F\colon \tilde{W}_s(K) \longrightarrow \tilde{W}_s(K)$ is the Frobenius morphism and, of course, this correspondence is an isomorphism of groups).

Taking the projective limit over s we obtain the isomorphism

$$\widetilde{W}(K)/(F - id)\widetilde{W}(K) \longrightarrow Hom_{cont}(\Gamma, \mathbf{Z}_p).$$

So, we have a full description of all $\mathbf{Z}_p$-extensions of K with an explicitly given action of the Galois group.

1.3.3. Let p be a fixed prime, $\mathcal{L}$ be a nilpotent finite dimensional Lie algebra over $\mathbb{F}_p$. We assume that the nilpotency class of $\mathcal{L}$ is less than p.

Let $A = A_{\mathcal{L}}$ be the envelopping algebra of $\mathcal{L}$. We remark that there exists a canonical embedding $\mathcal{L} \subset A$. For any field K of characteristic p the coalgebra structure on $A_K = A \otimes K$ is given uniquely by the conditions: $\Delta(l) = l \otimes 1 + 1 \otimes l$ and $\varepsilon(l) = 0$ for $l \in \mathcal{L}$. If $J(A_K) = Ker\varepsilon$, then we define the decreasing filtration

$\{J_s(A_K)\}$ of A_K for all $s \geq 0$ by $J_s(A_K) := J^s(A_K)$. It is easy to see, that A is an f.a.b.

Let

$$\widetilde{log}(T) = \sum_{1 \leq i \leq p-1} (-1)^{i-1}(T-1)^i/i$$

be the truncated logarithm. It is clear, that for $s < p$ the correspondence $a \mapsto \widetilde{log} a$ defines a one-to-one correspondence between the sets $1 + J_1(A_K) \bmod J_s(A_K)$ and $J_1(A_K) \bmod J_s(A_K)$.

Proposition. *For $s < p$, the correspondence $a \mapsto \widetilde{log} a$ defines one-to-one mapping between $G_K(s)$ and $\mathcal{L} \otimes K \bmod J_s(A_K)$.*

Proof. Let $\mathcal{L}_K = \mathcal{L} \otimes K$, $C_1(\mathcal{L}_K) = \mathcal{L}_K$, and, for $s > 1$, $C_s(\mathcal{L}_K) = [C_{s-1}(\mathcal{L}_K), \mathcal{L}_K]$. We have: $C_p(\mathcal{L}) = 0$ and, for any $s_1, s_2 \geq 1$, $[C_{s_1}(\mathcal{L}), C_{s_2}(\mathcal{L})] \subset C_{s_1+s_2}(\mathcal{L})$.

For any $l \in \mathcal{L}$ we set: $w(l) = max\{i | l \in C_i(\mathcal{L})\}$. Now choose a special basis $l_1, l_2, ..., l_N$ of $\mathcal{L}_K$ over K, where $dim_K \mathcal{L}_K = N$, satisfying the following condition:

$\{l_i | l_i \in C_s(\mathcal{L})\}$ is a K-basis of $C_s(\mathcal{L})$ for all $s < p$.

The equivalent condition:

$\{l_i | w(l_i) = s\}$ is a basis of the supplementary vector space for $C_{s+1}(\mathcal{L})$ in $C_s(\mathcal{L})$ for all $s < p$;

By the Birkhoff-Witt theorem the monomials $l_1^{a_1} l_2^{a_2} ... l_N^{a_N}$, where $a_i \in \mathbb{N} \cup \{0\}$ for $1 \leq i \leq N$, give a K-basis of A_K. We set $w(l_1^{a_1} l_2^{a_2} ... l_N^{a_N}) = \sum_{i=1}^{N} a_i w(l_i)$.

Lemma. *For any s the set $\{l_1^{a_1} l_2^{a_2} ... l_N^{a_N} \mid w(l_1^{a_1} l_2^{a_2} ... l_N^{a_N}) \geq s\}$ gives a basis of $J_s(A_K)$ over K.*

Proof. By definition $l \in J_{w(l)}(A_K)$ for any $l \in \mathcal{L}_K$. Hence, any monome $l_1^{a_1} l_2^{a_2} ... l_N^{a_N}$ of w-weight $\geq s$ is in $J_s(A_K)$. Conversely, the ideal $J(A_K) = Ker(\varepsilon)$ is generated by the set $\{l_i \mid w(l_i) = 1\}$. Therefore, it is sufficient to prove that every product $l_{i_1} ... l_{i_{s_1}}$, where $s_1 \geq s$, $1 \leq i_1, ..., i_{s_1} \leq N$, $w(l_{i_1}) = ... = w(l_{i_{s_1}}) = 1$, can be expressed as a sum of monomials $l_1^{a_1} l_2^{a_2} ... l_N^{a_N}$ which have w-weight $\geq s_1$. If $i_1 \leq i_2 \leq ... \leq i_{s_1}$ then $l_{i_1} ... l_{i_{s_1}}$ is one of these monomials of w-weight $s_1 \geq s$. So, here is nothing to prove. If the sequence of indices $i_1, i_2, ..., i_{s_1}$ does not grow, we must use the commutator relations for presenting $l_{i_1} ... l_{i_{s_1}}$ as a sum of monomials from the Birkhoff-Witt basis. These relations are of the following kind: $l' l'' = l'' l' + \sum_i \alpha_i l_i$, where $l', l'' \in \{l_1, l_2, ..., l_N\}$, all $\alpha_i \in K$ and $\alpha_i = 0$ if $w(l_i) < w(l') + w(l'')$ (this follows from the special choice of the basis $l_1, l_2, ..., l_N$). It is clear, that these relations are able to give us only monomials of the weight $\geq s_1$. The Lemma is proved.

We continue the proof of the proposition. Let $a \in G_K(s)$ and $\hat{a} \in A_K$ be such that $a = \hat{a} \mod J_{s+1}(A_K)$. Consider $b = \widetilde{log}(\hat{a})$. Then

$$\Delta b \equiv b \otimes 1 + 1 \otimes b \mod J_{s+1}(A_K \otimes A_K)$$

Let $b = \sum_{i \geq 1} b_i$, where every b_i is a linear combination of the monomials from the Birkhoff-Witt basis with the w-weight equal to i. We note that the elements

$l_1^{a_1} l_2^{a_2} \dots l_N^{a_N} \otimes l_1^{b_1} l_2^{b_2} \dots l_N^{b_N}$, where $a_i, b_i \in \mathbb{N} \cup \{0\}$ for $1 \le i \le N$, give the Birkhoff-Witt basis of the envelopping algebra of $\mathcal{L}_K \oplus \mathcal{L}_K$. Obviously, for any i, $\Delta(b_i) - (b_i \otimes 1 + 1 \otimes b_i)$ can be expressed as a linear combination of such monomials with the w-weight equal to i. So, we have: $\Delta(b_i) - (b_i \otimes 1 + 1 \otimes b_i)$ is equal to 0 or has w-weight equal to i. By the condition we have: $\Delta(b) - (b \otimes 1 + 1 \otimes b) \in J_{s+1}(A_K \otimes A_K)$. It follows now from the above lemma that

$$w(\Delta b - (b \otimes 1 + 1 \otimes b)) = w(\sum_{i \ge 1} (\Delta b_i - (b_i \otimes 1 + 1 \otimes b_i))) \ge s + 1.$$

Hence, for $i \le s$ we have $\Delta b_i = b_i \otimes 1 + 1 \otimes b_i$. This means that $b_i \in \mathcal{L}_K$ for $i \le s$, c.f.[B], and the proposition is proved.

Corollary. *The f.a.b. A satisfies the condition (C_{p-1}).*

By means of the characteristic p-case of the Campbell-Hausdorff formula (c.f.[B]) we can conclude:

Corollary. *The correspondence $\mathcal{L} \mapsto G_{\mathbb{F}_p}(\mathcal{L})$ gives us an equivalence of the category of Lie $\mathbb{F}_p$-algebras with class of nilpotency $< p$ and the category of p-periodic groups with class of nilpotency $< p$.*

After these preparations we are able to apply theorem n.1.2 to the explicit description of the Galois extensions of K with arbitrary p-periodic Galois group of nilpotency class $< p$.

Let $e \in G_K(s)$, $s < p$ and $\tilde{\pi}_s(e)$ be the corresponding conjugacy class in $Hom(\Gamma, G_{\mathbb{F}_p}(s))$. Let $l_1, \dots, l_n$ be the part of the special basis of $\mathcal{L}$ from the above proposition which consists of the elements with w-weight equal to 1. Then for the reduction $r_{s,1}(e)$ of e we have: $r_{s,1}(e) = 1 + w_1 l_1 + \dots + w_n l_n \mod J_2(A_K)$, where $w_1, \dots, w_n \in K$.

Proposition. *The conjugacy class $\tilde{\pi}_s(e)$ consists of epimorphisms iff the images of $w_1, \dots, w_n$ in $K/(F - id)K$ are linearly independent (here F is the Frobenius morphism of K).*

Proof. For $s = 1$ it can be easily checked by the usual Artin-Shreier theory.

Let $s > 1$, $f : \Gamma \longrightarrow G_{\mathbb{F}_p}(s)$ be any homomorphism from the class $\tilde{\pi}_s(e)$. $G_{\mathbb{F}_p}(s)$ is a p-group, hence f factors through the quotient $\Gamma \longrightarrow \Gamma(p)$, where $\Gamma(p)$ is the Galois group of the maximal p-extension of K. As the one-to-one correspondences π_s and π_1 from our theorem agree one with another under the reduction mapping $r_{s,1}$ we can conclude that the composition $\Gamma(p) \longrightarrow G_{\mathbb{F}_p}(s) \longrightarrow G_{\mathbb{F}_p}(1)$ is an epimorphism. But

$$Ker(G_{\mathbb{F}_p}(s) \longrightarrow G_{\mathbb{F}_p}(1)) = [G_{\mathbb{F}_p}(s), G_{\mathbb{F}_p}(s)]$$

so our proposition follows from the well-known property of p-groups:

let Γ_1, Γ_2 be profinite p-groups, then the homomorphism $\pi : \Gamma_1 \longrightarrow \Gamma_2$ is an epimorphism iff it induces an epimorphism

$$\Gamma_1 / \Gamma_1^p [\Gamma_1, \Gamma_1] \longrightarrow \Gamma_2 / \Gamma_2^p [\Gamma_2, \Gamma_2]$$

c.f.[Se2], Ch.1, n.4.

Example. In order to illustrate the above considerations we apply them to explicit construction of extensions of K with noncommutative Galois groups of order p^3 for $p > 2$. Let $\mathcal{L}$ be a Lie algebra over $\mathbb{F}_p$ with $\mathbb{F}_p$-basis l_1, l_2, l_3 and relations $[l_1, l_2] = l_3, [l_1, l_3] = [l_2, l_3] = 0$. We assume that $w_1, w_2 \in K$ have linearly independent images in the quotient $K/(F - id)K$ and take a 2-diagonal element $e = E \mod J_2(A_K)$, where $E = \widetilde{exp}(w_1 l_1 + w_2 l_2)$. The corresponding extension $L = K(T_1, T_2, T_3)$ of K is given by $\mathcal{F}^{(p)} \equiv \mathcal{F}E \mod J_3(A_{K_{sep}})$, where $\mathcal{F} = \widetilde{exp}(T_1 l_1 + T_2 l_2 + T_3 l_3)$.

By the Campbell-Hausdorff formula we obtain:

$$\begin{aligned}
&\widetilde{exp}(T_1^p l_1 + T_2^p l_2 + T_3^p l_3) \equiv \\
&\quad \equiv \widetilde{exp}(T_1 l_1 + T_2 l_2 + T_3 l_3)\widetilde{exp}(w_1 l_1 + w_2 l_2) \equiv \\
&\quad \equiv \widetilde{exp}((T_1 + w_1) l_1 + (T_2 + w_2) l_2 + (w_2 T_1/2 - w_1 T_2/2 + T_3) l_3).
\end{aligned}$$

Now we have the explicit equations of this extension:

$$T_1^p = T_1 + w_1, T_2^p = T_2 + w_2, T_3^p = T_3 + (w_2 T_1 - w_1 T_2)/2.$$

The action of $Gal(L/K) \simeq G_{\mathbb{F}_p}(2)$ is given by the relation $\mathcal{F} \mapsto u\mathcal{F}$, $u \in G_{\mathbb{F}_p}(2)$. For example, the generators $u_1 = \widetilde{exp}(l_1)$ and $u_2 = \widetilde{exp}(l_2)$ of $G_{\mathbb{F}_p}(2)$ act in the following manner:

$$u_1 : (T_1, T_2, T_3) \mapsto (T_1 + 1, T_2, T_3 + T_2/2)$$
$$u_2 : (T_1, T_2, T_3) \mapsto (T_1, T_2 + 1, T_3 - T_1/2)$$

2. Explicit construction of the Galois action (the case of a general field).

2.1. Let K be a field of characteristic $p > 0$, $\Gamma_K = Gal(K_{sep}/K)$, let $\mathcal{L}$ be a finite dimensional Lie algebra over $\mathbf{F}_p$ and A be the envelopping algebra of $\mathcal{L}$ with the structure of an f.a.b.,defined in n.1.3. We shall use the notations of n.1.3.

Let $s_0 < p$, $e \in G_K(s_0)$, $M_{s_0}(e) = \{f \in G_{K_{sep}}(s_0) | f^{(p)} = fe\}$ be the set from the proof of theorem 1.2. We denote by d: $A \longrightarrow \mathbf{N}$ the grading of A and by $\{c_\alpha\}_{\alpha \in I}$ the special $\mathbf{F}_p$-basis of A which were defined in the proof of lemma 1.2.1.

Let $f \in M_{s_0}(e)$. We can take its (uniquely defined) representative

$$\hat{f} = 1 + \sum_{d(c_\alpha) \le s_0} f_\alpha c_\alpha$$

in $A_{K_{sep}}$ and denote by $\mathcal{M}_{s_0}(e)$ the $\mathbf{F}_p$-submodule in K_{sep} generated by all f_α with $d(c_\alpha) \le s_0$.

We have:

2.1a. $\mathcal{M}_{s_0}(e)$ does not depend on the choice of the special basis $\{c_\alpha\}_{\alpha \in I}$. Also it does not depend on the choice of $f \in M_{s_0}(e)$.

2.1b. $\mathcal{M}_{s_0}(e)$ is the Γ_K-invariant submodule of K_{sep}.

2.1c. If the homomorphism $F : \Gamma_K \longrightarrow Aut\mathcal{M}_{s_0}(e)$ gives us an action of Γ_K on $\mathcal{M}_{s_0}(e)$ then $Ker F = Gal(K_{sep}/K_{s_0}(e))$, where $K_{s_0}(e)$ is the minimal extension of

K in K_{sep} such that the following implication is true: $f \in M_{s_0}(e) \Rightarrow f \in G_{K_{s_0}}(s_0)$, c.f.1.2.

2.1d. For any $\tau \in \Gamma_K$, $F(\tau)$ is a unipotent automorphism of $\mathcal{M}_{s_0}(e)$ such that $(F(\tau) - id)^{s_0+1} = 0$. Therefore it defines an endomorphism $L(\tau) = \widetilde{log} F(\tau) \in End\mathcal{M}_{s_0}(e)$.

Let the representative $\hat{e}$ of e be of the form

$$\hat{e} = 1 + \sum_{d(c_\alpha) \leq s_0} e_\alpha c_\alpha$$

and suppose that the images of elements of the set $\{e_\alpha | \alpha \in I, d(c_\alpha) = 1\}$ in $K/(K - id)$ are linearly independent. We fix $f \in M_{s_0}(e)$. Then the homomorphism $\pi_{e,f,s_0} : \Gamma_K \longrightarrow G_{\mathbf{F}_p}(s_0)$ from 1.2.5 is an epimorphism and defines an isomorphism $Gal(K_{s_0}(e)/K) \simeq G_{\mathbf{F}_p}(s_0)$. By proposition 1.1.3, for any $\tau \in \Gamma_K$ there exists a unique $l_\tau \in \mathcal{L}$ such that $\pi_{e,f,s_0}(\tau) = \widetilde{exp}(l_\tau) \mod J_p(A)$.

We have:

2.1e. The correspondence $l_\tau \mapsto L(\tau)$ for $\tau \in \Gamma_K$ (c.f. 2.1d) defines a homomorphism of Lie algebras $LF : \mathcal{L} \longrightarrow End\mathcal{M}_{s_0}(e)$, i.e. gives the action of the Lie algebra $\mathcal{L}$ on $\mathcal{M}_{s_0}(e)$.

2.2. Let us treat the previous construction in the case of a free Lie algebra and $s_0 = p - 1$.

So, let $\mathcal{L}$ be a free Lie algebra over $\mathbf{F}_p$ with free generators $D_1, ..., D_N$. We can take the system

$$\{D_{i_1} ... D_{i_s} | 1 \leq i_1, ..., i_s \leq N, s \geq 1\}$$

as a special basis $\{c_\alpha\}_{\alpha \in I}$. It is easy to see that if $\mathcal{G}$ is a free group with free generators $g_1, ..., g_N$ then the correspondence $g_i \mapsto \widetilde{exp}\ (D_i) mod J_p(A)$, where $i = 1, ..., N$, defines an epimorphism $h : \mathcal{G} \longrightarrow G_{\mathbf{F}_p}\ (p-1)$ and $Ker h = \mathcal{G}^p C_p(\mathcal{G})$, where $C_p(\mathcal{G})$ is the subgroup of $\mathcal{G}$, generated by all commutators of length p.

Let $w_1, ..., w_N \in K$ be such that their images in $K/(F - id)K$ are linearly independent. If we take

$$e = \widetilde{exp}(\sum_{1 \leq i \leq N} w_i D_i) \mod J_p(A_K) \in G_K(p-1)$$

then

$$\hat{e} = 1 + \sum_{\substack{1 \leqslant s < p \\ i_1, ..., i_s}} \frac{1}{s!} w_{i_1} ... w_{i_s} D_{i_1} ... D_{i_s}$$

Let $f \in M_{p-1}(e)$ and

$$\hat{f} = 1 + \sum_{\substack{1 \leqslant s < p \\ i_1, ..., i_s}} T_{i_1, ..., i_s} D_{i_1} ... D_{i_s}$$

Then the elements $T_{i_1, ..., i_s}$, where $1 \leq s < p$, $1 \leq i_1, ..., i_s \leq N$, generate $\mathcal{M}_{p-1}(e)$ and the equality $f^{(p)} = fe$ gives the following equations for these elements

$$T^p_{i_1,\dots,i_s} = T_{i_1\dots i_s} + T_{i_1\dots i_{s-1}}\frac{w_{i_s}}{1!} + \dots + \frac{w_{i_1}\dots w_{i_s}}{s!}$$

The action of the Lie algebra $\mathcal{L}$ on $\mathcal{M}_{p-1}(e)$ is given by the relations

$$LF(D_i)(T_{i_1\dots i_s}) = \delta(i,i_1)T_{i_2\dots i_s}$$

for any $1 \le i, i_1, \dots, i_s \le N, 1 \le s < p$, where $\delta(i,i_1)$ is the Kronecker symbol. It gives the faithful action of $\widetilde{\mathcal{L}} = \mathcal{L}/C_p(\mathcal{L})$ on $\mathcal{M}_{p-1}(e)$ (where $C_p(\mathcal{L})$ is the ideal in $\mathcal{L}$ generated by all commutators having length p).

We can identify $Gal(K_{p-1}(e)/K)$ and $G_{\mathbb{F}_p}(p-1)$ by means of $\pi_{e,f,p-1}$. Then we have the explicit description of the Galois action, which is given on generators $\tau_i = \widetilde{exp}(D_i) \mod J_p(A), 1 \le i \le n$ by the following relation:

$$\tau_i(T_{i_1\dots i_s}) = T_{i_1\dots i_s} + \frac{1}{1!}\delta(i,i_1)T_{i_2\dots i_s} + \frac{1}{2!}\delta(i,i_1,i_2)T_{i_3\dots i_s} + \dots$$

where $\delta(i,i_1,\dots,i_l)$ is equal to 1 if $i = i_1 = \dots i_l$ and is equal to 0 otherwise.

Proposition. *The system* $\{T_{i_1\dots i_s} | 1 \leqslant s < p, 1 \le i_1, \dots, i_s \le N\}$ *is linearly independent over* K.

Proof. Let

$$\sum_{\substack{1\leqslant s<p\\ i_1\dots i_s}} \alpha_{i_1\dots i_s} T_{i_1\dots i_s} = 0$$

be any nontrivial linear relation. Let us choose the $\alpha_{i_{1'}\dots i'_{s'}} \ne 0$ with the largest s'. Then the relation

$$LF(D_{i'_1})\dots LF(D_{i'_{s'}})(\sum \alpha_{i_1\dots i_s}T_{i_1\dots i_s}) = \alpha_{i'_1\dots i'_{s'}}$$

gives us a contradiction.

2.3. We can give the following profinite version of the previous construction.

Let $V \subset K$ be a $\mathbb{F}_p$-subspace, such that $V + (F-id)K = K$ and $V \cap (F-id)K = 0$, where $F : K \longrightarrow K$ is the absolute Frobenius map on K. Let us choose an $\mathbf{F}_p$-basis $\{w_i\}_{i\in I}$ of V.

For any finite subset $R \subset I$ we denote by V_R the subspace of V which is generated by w_i, $i \in R$. Obviously, $V = \varinjlim V_R$. Let $V_R^* = Hom(V_R, \mathbb{F}_p)$ be the dual vector space for V_R. Then $V^* = \varprojlim V_R^*$ is the topological vector space over $\mathbb{F}_p$ dual to V. Let us denote by $\{D_i\}_{i\in I}$ the topological $\mathbf{F}_p-$ basis of V^* dual to the basis $\{w_i\}_{i\in I}$.

For any finite subset $R \subset I$ we denote by $\mathcal{L}_R$ the free Lie algebra with the system of (free) generators $\{D_i\}_{i\in R}$. Then $\mathcal{L} = \varprojlim \mathcal{L}_R$ is a profinite free Lie algebra over $\mathbb{F}_p$ with the module of free generators V^*. Let A_R be the envelopping algebra of $\mathcal{L}_R$, then $A = \varprojlim A_R$ is the (topological) envelopping algebra of $\mathcal{L}$. We assume that all A_R and A are equipped with the structure of f.a.b (c.f. 1.3.1). We also shall use the notation of n.1.3 for all constructions related to A. The notation for all similar constructions related to A_R will be equipped with the indice R.

Let

$$e_R = \widetilde{exp}(\sum_{i\in R} w_iD_i) \bmod J_p(A_{K,R}) \in G_{K,R}(p-1)$$

and $e = \varprojlim_R e_R \in G_K(p-1)$. Choose $f \in \varprojlim_R M_{p-1}(e_R)$ and denote by f_R the projections of f to $M_{p-1}(e_R)$ for any finite subset $R \subset I$. Then we have a system of epimorphisms $\pi_{e,f,p-1,R} : \Gamma_K \longrightarrow G_{\mathbb{F}_p,R}\ (p-1)$ which gives an epimorphism $\pi_f := \varprojlim_R \pi_{e,f,p-1,R} : \Gamma_K \longrightarrow G_{\mathbb{F}_p}(p-1)$. It is clear that π can be factored through the quotient $\Gamma_K \longrightarrow \Gamma_K(p)$, where $\Gamma_K(p)$ is the Galois group of the maximal p-extension $K(p)$ of K. It is well known, c.f.[Se2, ch.2, n.2], that $\Gamma(p)$ is a free pro$-p$-group and from [Se2, Ch.1, n.4] we obtain that π defines an epimorphism $\pi_f(p)\colon \Gamma(p) \longrightarrow G_{\mathbb{F}_p}(p-1)$ such that $\mathrm{Ker}\,\pi_f(p) = \Gamma^p(p)C_p(\Gamma(p))$.

Let

$$\hat{f} = 1 + \sum_{\substack{1\leqslant s<p\\ i_1,\dots,i_s\in I}} T_{i_1\dots i_s}D_{i_1}\dots D_{i_s}$$

be the representative of f. Then we have:

2.3a. *All $T_{i_1\dots i_s}$ are in $K(p)^{\Gamma^p(p)C_p(\Gamma(p))}$.*

2.3b. *The system $\{T_{i_1\dots i_s} | 1 \le s < p, i_1, \dots, i_s \in I\}$ is linearly independent over K.*

2.3c. *The $\mathbb{F}_p$-module $\mathcal{M}$ generated by all $T_{i_1\dots i_s}$ is invariant by the Galois action.*

2.3d. *There is an action of the profinite Lie algebra $\mathcal{L}$ on $\mathcal{M}$, $LF : \mathcal{L} \longrightarrow End\mathcal{M}$, given by the following relation on free generators D_i, $i \in I$:*

$$LF(D_i)(T_{i_1\dots i_s}) = \delta(i, i_1)T_{i_2\dots i_s}.$$

Let $T(w_{i_1}, \dots, w_{i_s}) = T_{i_1\dots i_s}$, where $1 \le s < p, i_1, \dots, i_s \in I$. Define $T(v_1, \dots, v_s) \in \mathcal{M}$ for $v_1, \dots, v_s \in V$ by multilinearity: if $v_i = \sum_{j\in J} \alpha_{ij}w_j$, for $i = 1, \dots, s$, where $\alpha_{ij} \in \mathbb{F}_p$ and almost all are equal to 0, then

$$T(v_1, \dots, v_s) = \sum_{j_1,\dots,j_s} \alpha_{1j_1}\dots\alpha_{sj_s}T(w_{j_1}, \dots, w_{j_s})$$

In this notation we have:

2.3e. $\mathcal{M} = \oplus_{1\le s<p}\mathcal{M}_s$ *where* $\mathcal{M}_s = \{T(v_1, \dots, v_s)|v_1, \dots, v_s \in V\}$

2.3f. *If $D \in V^*$ then*

$$LF(d)(T(v_1, \dots, v_s)) = \langle D, v_1\rangle T(v_2, \dots, v_s)$$

for any $v_1, \dots, v_s \in V$.

2.3g. *$T(v_1, \dots, v_s)$ satisfy the following equation:*

$$T(v_1, \dots, v_s)^p = T(v_1, \dots, v_s) + \frac{v_1}{1!}T(v_2, \dots, v_s) + \dots + \frac{v_1\dots v_s}{s!}$$

2.3h. *Let $\tau \in \Gamma_K$ and $l_\tau \in \mathcal{L}$ be such that*

$$\pi_f(\tau) = \widetilde{exp}(l_\tau)modJ_p(A).$$

Then l_τ is uniquely defined modulo $C_p(\mathcal{L})$ and $\tau|_{\mathcal{M}} = \widetilde{exp}(LF(l_\tau))$.

3. Explicit construction of the Galois action (the case of a local field).

Let k be a local field of characteristic $p > 0$, complete with respect to a discrete valuation and with residue field $k \simeq \bar{\mathbb{F}}_p$. Then K is isomorphic to the fraction field of the power series ring over k. We fix some uniformising element of this ring in the form t^{-1}, $t \in K$.

We shall give some modification of the previous construction which will be useful later in the study of the ramification filtration.

3.1. Structural element e° and constants $\eta(r_1, ..., r_s)$.
Let

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

For any finite subset $R \subset \mathbb{Q}^+(p)$ consider a free Lie $\mathbb{F}_p$-algebra $\mathcal{L}_R^\circ$ having a set of free generators $\{D_r^\circ | r \in R\}$. Then $\varprojlim_R \mathcal{L}_R^\circ = \mathcal{L}^\circ$ is a pro-free Lie $\mathbb{F}_p$-algebra with the set of free generators $\{D_r^\circ | r \in \mathbb{Q}^+(p)\}$. If A_R is an f.a.b. related to $\mathcal{L}_R^\circ$ then $A^\circ = \varprojlim_R A_R^\circ$ is an f.a.b. related to $\mathcal{L}^\circ$.

We call an element $e^\circ \in A^\circ \bmod J_p(A^\circ)$ *structural* if

(1) $e^\circ \in G_{A^\circ, \mathbb{F}_p}(p-1)$
(2) $e^\circ \equiv 1 + \sum_{r \in \mathbb{Q}^+(p)} D_r^\circ \mod J_2(A^\circ)$

It is clear that $e^\circ = \varprojlim_R e_R^\circ$, where $e_R^\circ \in G_{A^\circ, \mathbb{F}_p}(p-1)$ and $e_R^\circ \equiv 1 + \sum_{r \in R} D_r^\circ \mod J_2(A_R^\circ)$.

As before we can consider a uniquely defined representative $E^\circ \in A_R^\circ$ of e° of the form

$$E^\circ = 1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in \mathbb{Q}^+(p)}} \eta(r_1, ..., r_s) D_{r_1}^\circ ... D_{r_s}^\circ$$

where $\eta(r_1, ..., r_s) \in \mathbb{F}_p$ for any $r_1, ..., r_s \in \mathbb{Q}^+(p)$.

These constants $\eta(r_1, ..., r_s)$ will be called the *structural* constants (related to a structural element e°).

Examples.

(1) If we take

$$E^\circ = \widetilde{exp}\Big(\sum_{r \in \mathbb{Q}^+(p)} D_r^\circ\Big)$$

then $e^\circ = E^\circ \bmod J_p(A^\circ)$ is a structural element and for its structural constants we have:

$$\eta(r_1, ..., r_s) = \frac{1}{s!}.$$

(2) If we take

$$E^\circ = \prod_{r \in \mathbb{Q}^+(p)} \widetilde{exp}(D_r^\circ)$$

with respect to the natural ordering in $\mathbb{Q}^+(p)$, then $e^\circ = E^\circ mod J_p(A^\circ)$ is structural and its structural constants are given by the following equalities:

$$\eta(r_1, ..., r_s) = \frac{1}{s_1!(s_2 - s_1)!...(s_l - s_{l-1})!},$$

if $r_1 = ... = r_{s_1} < r_{s_1+1} = ... = r_{s_2} < ... < r_{s_{l-1}+1} = ... = r_{s_l}$,where $1 \leq s_1 < s_2 < ... < s_l = s$, and

$$\eta(r_1, ..., r_s) = 0$$

otherwise, i.e. if $r_1 \leq r_2 \leq ... \leq r_s$ is not true.

Proposition. *A collection of constants $\eta(r_1, ..., r_s) \in \mathbb{F}_p$, where $r_1, ...r_s \in \mathbb{Q}^+(p)$, $1 \leq s < p$, is a collection of structural constants iff:*

(1) *for any $r_1 \in \mathbb{Q}^+(p)$, $\eta(r_1) = 1$;*

(2) *if s_1, s_2 are natural numbers such that $s = s_1 + s_2 < p$ then*

$$\eta(r_1, ...r_{s_1})\eta(r_{s_1+1}, ..., r_{s_2}) = \sum_{\sigma \in P_{s_1,s_2}} \eta(r_{\sigma(1)}, ..., r_{\sigma(s_2)}),$$

where P_{s_1,s_2} is the subset of permutations of order s_2 such that $\sigma(i) < \sigma(j)$, where $1 \leq i < j \leq s_1$ or $s_1 + 1 \leq i < j \leq s_2$.

Proof. It follows from the fact that in the coalgebra A° we have:

$$\Delta(D_{r_1}...D_{r_{s_2}}) = \sum_{\substack{0 \leqslant s_1 \leqslant s_2 \\ \sigma \in P_{s_1,s_2}}} D_{r_{\sigma^{-1}(1)}}...D_{r_{\sigma^{-1}(s_1)}} \otimes D_{r_{\sigma^{-1}(s_1+1)}}...D_{r_{\sigma^{-1}(s_2)}}$$

We assume until the end of this paper, that some structural element e° and its structural constants $\eta(r_1, ..., r_s)$, where $1 \leq s < p, r_1, ..., r_s \in \mathbb{Q}^+(p)$, are fixed.

3.2. Let K_{sep} be any fixed separable closure of K, $\Gamma = \Gamma_K = Gal(K_{sep}/K)$. For any natural number N we consider the extension $K_N = K(t_N) \subset K_{sep}$, where $t_N^{p^N-1} = t$. The system of these fields K_N is an inductive system of the subfields in K_{sep} and $\varinjlim_N K_N = K_{tr}$ is the maximal tamely ramified extension of K. Now K_{sep} can be considered as a maximal p-extension of K_{tr}. Its Galois group $I = Gal(K_{sep}/K_{tr})$ is called the subgroup of higher ramification of Γ and as was mentioned earlier is a free pro-p-group.

In order to apply the construction of n.2.3 we can assume that elements $t_N \in K_{tr}, N \geq 1$, satisfy the following condition: for any natural numbers N_1, N_2 such that $N_2|N_1$ we have: $t_{N_2} = t_{N_1}^{1+p^{N_2}+...+p^{(l-1)N_2}}$, where $N_1 = lN_2$.

Let $\mathbb{Q}^+(p)$ be the set defined in n.3.1. Obviously, every $r \in \mathbb{Q}^+(p)$ can be written in the form $r = \frac{m}{p^N-1}$ with some natural numbers m, N, where $(m,p) = 1$. We use this fact to define $t^r := t_N^m$ for $r \in \mathbb{Q}^+(p)$. It is easy to see that this definition does not depend on the above choice of m and N.

Now consider the vector space

$$V = \bigoplus_{r \in \mathbb{Q}^+(p)} kt^r \subset K_{tr}$$

over $\mathbb{F}_p$, then $V + (F - id)K_{tr} = K_{tr}$ and $V \cap (F - id)K_{tr} = 0$, where $F : K \longrightarrow K$ is the absolute Frobenius endomorphism of K. Let $\{w_i\}_{i \in I}$ be some basis of k over $\mathbb{F}_p$, then

$$\{w_i t^r | i \in I, r \in \mathbb{Q}^+(p)\}$$

is an $\mathbf{F}_p$-basis of V. As earlier we consider the dual vector space

$$V^* = Hom(V, \mathbf{F}_p) = \prod_{r \in \mathbb{Q}^+(p)} Hom(k, \mathbf{F}_p)_r$$

for V and the profinite free Lie algebra $\mathcal{L}$ with the $\mathbb{F}_p$-module of free generators V^*.

Let

$$E^\circ = 1 + \sum \eta(r_1, ..., r_s) D^\circ_{r_1} ... D^\circ_{r_s}$$

be a representative of a fixed structural element e°(c.f. 3.1). We write $E^\circ = E^\circ(\{D^\circ_r\}_{r \in \mathbb{Q}^+(p)})$ if we want to consider E° as a function of variables D°_r, $r \in \mathbb{Q}^+(p)$.

Consider the element

$$E = E^\circ(\{\sum_{i \in I} w_i t^r D_{i,r}\}_{r \in \mathbb{Q}^+(p)})$$

of $A_{K_{tr}} = A \otimes K_{tr}$, where A is an f.a.b. related to $\mathcal{L}$, and

$$\{D_{i,r} | i \in I, r \in \mathbb{Q}^+(p)\}$$

is a basis of V^* dual to basis

$$\{w_i t^r | i \in I, r \in \mathbb{Q}^+(p)\}$$

of V.

It is clear that E does not depend on the choice of basis $\{w_i | i \in I\}$ of k over $\mathbb{F}_p$, $e = E \mod J_p(A_{K_{tr}}) \in G_{K_{tr}}(p-1)$ and

$$E \equiv 1 + \sum_{\substack{1 \leqslant s < p \\ i_1, ..., i_s \in I \\ r_1, ..., r_s \in \mathbb{Q}^+(p)}} \eta(r_1, ..., r_s) w_{i_1} ... w_{i_s} t^{r_1 + ... + r_s} D_{i_1 r_1} ... D_{i_s r_s}.$$

3.3. Let $\widetilde{K} = K_{sep}^{I^p C_p(I)}$. As earlier we have:

3.3a. *The set*

$$\{T_{i_1 r_1 ... i_s r_s} | i_1, ..., i_s \in I, r_1, ..., r_s \in \mathbb{Q}^+(p), 1 \leq s < p\}$$

generates an I-invariant $\mathbf{F}_p$-submodule $\mathcal{M}$ in $\widetilde{K}$. This set is linearly independent over K_{tr} (therefore, this set is $\mathbf{F}_p$-basis of $\mathcal{M}$).

3.3b. *The elements* $T_{i_1r_1...i_sr_s}$, *where* $i_1,...,i_s \in I, r_1,...,r_s \in \mathbb{Q}^+(p), 1 \le s < p$, *satisfy the relations*

$$T^p_{i_1r_1...i_sr_s} = T_{i_1r_1...i_sr_s} + T_{i_1r_1...i_{s-1}r_{s-1}} w_{i_s} t^{r_s}\eta(r_s) + ... + w_{i_1}...w_{i_s} t^{r_1+...+r_s}\eta(r_1,...,r_s).$$

3.3c. *The Lie algebra* $\mathcal{L}$ *acts on* $\mathcal{M}$ *and this action* $LF : \mathcal{L} \longrightarrow End\mathcal{M}$ *is given on its generators* $D_{i,r}, i \in I, r \in \mathbb{Q}^+(p)$ *by the relation*

$$L(D_{i,r})(T_{i_1r_1...i_sr_s}) = \delta(i,i_1)\delta(r,r_1)T_{i_2r_2...i_sr_s}.$$

3.3d. *For any* $\tau \in I$ *there exists* $l_\tau \in \mathcal{L}$, *uniquely defined modulo* $C_p(\mathcal{L})$, *such that* $\tau|_{\mathcal{M}} = \widetilde{exp}LF(l_\tau)$.

As earlier we define $T_{i_1r_1...i_sr_s} = T(w_{i_1},r_1,...,w_{i_s},r_s)$ for all $i_1,...,i_s \in I$, $r_1,...,r_s \in \mathbb{Q}^+(p), 1 \le s < p$ and define elements $T(\alpha_1,r_1,\ ...,\alpha_s,r_s) \in \mathcal{M}$ for any $\alpha_1,...,\alpha_s \in k$ by multilinearity. We have:

for any $\alpha_1,...,\alpha_s \in k, r_1,...,r_s \in \mathbb{Q}^+(p)$:

3.3e.

$$T(\alpha_1,r_1,...,\alpha_s,r_s)^p = T(\alpha_1,r_1,...,\alpha_s,r_s)+$$

$$+T(\alpha_1,r_1,...,\alpha_{s-1},r_{s-1})\alpha_s t^{r_s}\eta(r_s) + ... + \alpha_1...\alpha_s t^{r_1+...+r_s}\eta(r_1,...,r_s)$$

3.3f. *If* $D = (D(r))_{r\in\mathbb{Q}^+(p)} \in V^* = \prod_{r\in\mathbb{Q}^+(p)} Hom(k,\mathbb{F}_p)_r$

then

$$LF(D)(T(\alpha_1,r_1,...,\alpha_s,r_s)) = \langle D(r_1),\alpha_1\rangle T(\alpha_2,r_2,\ ...,\alpha_s,r_s).$$

Remark.

We obtain a similar description for part of the maximal p-extension of K if everywhere we replace K_{tr} by K and $\mathbb{Q}^+(p)$ by $\mathbb{Z}^+(p) = \{n \in \mathbb{N} | (n,p) = 1\}$.

4.The "ramification" filtration of the Lie algebra $\mathcal{L}$.

Let $\mathcal{L}$ be the profinite free Lie algebra over $\mathbb{F}_p$ defined in n.2.3 and $\widetilde{\mathcal{L}} = \mathcal{L}/C_p(\mathcal{L})$, where $C_p(\mathcal{L})$ is the ideal of $\mathcal{L}$ generated by all commutators of length p. We define in this section a decreasing filtration $\{\widetilde{\mathcal{L}}^{(v)}\}_{v>0}$ of $\widetilde{\mathcal{L}}$ by its ideals $\widetilde{\mathcal{L}}^{(v)}$, where $v \in \mathbb{Q}, v > 0$. This filtration will be related to the ramification filtration of the $Gal(K_{sep}/K)$ in n.7 below. We use the notation of n.3.

4.1. Let $V = \bigoplus_{r\in\mathbb{Q}^+(p)} kt^r \subset K_{tr}$ be the vector space over $\mathbb{F}_p$ from n.2.4. For any finite subset R in $\mathbb{Q}^+(p)$ and natural number N we introduce the vector space $V_{R,N} = \bigoplus_{r\in R} \mathbb{F}_q t^r$ over $\mathbb{F}_p$, where $q = p^N$. Obviously, each $V_{R,N}$ can be identified with a subspace in V and $V = \varinjlim_{R,N} V_{R,N}$. Let $\mathcal{L}_{R,N}$ be a free Lie algebra over $\mathbb{F}_p$ with an $\mathbb{F}_p$-module of free generators $V^*_{R,N} = Hom(V_{R,N},\mathbb{F}_p)$. Then $\{\mathcal{L}_{R,N}\}_{R,N}$ is a projective system and $\varprojlim_{R,N} \mathcal{L}_{R,N} = \mathcal{L}$, where $\mathcal{L}$ is the free profinite Lie algebra over $\mathbb{F}_p$ from n.2.4. We set also $\widetilde{\mathcal{L}}_{R,N} = \mathcal{L}_{R,N}/C_p(\mathcal{L}_{R,N})$. It is clear that $\varprojlim \widetilde{\mathcal{L}}_{R,N} = \widetilde{\mathcal{L}}$.

4.2. The elements $D_\lambda(r_1,0,r_2,m_2,...,r_s,m_s)$ of $\mathcal{L}_{R,N}$.

Let $N\geq 1$, $q=p^N$. Then

$$Hom(\mathbb{F}_q,\mathbb{F}_p)\subset Hom(\mathbb{F}_q\otimes\mathbb{F}_q,\mathbb{F}_q)=\bigoplus_{n mod N} Hom_n(\mathbb{F}_q,\mathbb{F}_q)$$

where $Hom_n(\mathbb{F}_q,\mathbb{F}_q)$ consists of all additive morphisms $\varphi:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ such that $\varphi(\alpha)=\alpha^{p^n}\varphi(1)$ for any $\alpha\in\mathbb{F}_q$. Now any $f\in Hom(\mathbb{F}_q,\mathbb{F}_p)$ can be identified with the sum $\sum\limits_{n \bmod N} f_n$ where all $f_n\in Hom_n(\mathbb{F}_q,\mathbb{F}_q)$ and the conjugacy condition $f_{n+1}=f_n^p$ holds for all $n \bmod N$. We note that for any $f\in Hom(\mathbb{F}_q,\mathbb{F}_p)$ there exists a unique $\beta_f\in\mathbb{F}_q$ such that $f(\alpha)=Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_f)$ for any $\alpha\in\mathbb{F}_q$. It is easy to see that in the above decomposition $f=\sum\limits_n f_n$, we have $f_n(1)=\beta_f^{p^n}$.

In the same way we can consider tensors $F\in Hom(\mathbb{F}_q^{\otimes s},\mathbb{F}_p)$ where s is any natural number. Such an F may be identified with the sum

$$\sum_{\text{all } n_i \bmod N} F_{n_1\ldots n_s}$$

where

$$F_{n_1\ldots n_s}\in Hom_{n_1,\ldots,n_s}(\mathbb{F}_q^{\otimes s},\mathbb{F}_q)$$

and $Hom_{n_1,\ldots,n_s}(\mathbb{F}_q^{\otimes s},\mathbb{F}_q)$ is a group of multilinear mappings such that

$$F_{n_1\ldots n_s}(\alpha_1,\ldots,\alpha_s)=\alpha_1^{p^{n_1}}\ldots\alpha_s^{p^{n_s}}F_{n_1\ldots n_s}\ (1,\ldots,1)$$

for all $\alpha_i\in\mathbb{F}_q$ and the conjugation conditions $F^p_{n_1\ldots n_s}=F_{n_1+1,\ldots,n_s+1}$ hold. If $F=f_1\otimes\ldots\otimes f_s$ for $f_i\in Hom(\mathbb{F}_q,\mathbb{F}_p), 1\leq i\leq s$, then $F_{n_1\ldots n_s}(1,\ldots,1)=\beta_{f_1}^{p^{n_1}}\ldots\beta_{f_s}^{p^{n_s}}$.

Let $\lambda\in\mathbb{F}_q$ and $m_2^\circ,\ldots,m_s^\circ$ be any integers such that $0\leq m_2^\circ,\ldots,m_s^\circ<N$. We shall use the same notation for their residues mod N. Using the above considerations we introduce a tensor

$$F_\lambda(m_2^\circ,\ldots,m_s^\circ)\in Hom(\mathbb{F}_q^{\otimes s},\mathbb{F}_p)$$

defined by the following conditions:

$$F_\lambda(m_2^\circ,\ldots,m_s^\circ)_{0,m_2^\circ,\ldots,m_s^\circ}(1,\ldots,1)=\lambda$$

and

$$F_\lambda(m_2^\circ,\ldots,m_s^\circ)_{0,m_2,\ldots,m_s}=0$$

for any residues $m_2,\ldots,m_s \bmod N$ such that $(m_2,\ldots,m_s)\neq(m_2^\circ,\ldots,m_s^\circ)$.

The above tensor can be expressed as a sum of elementary tensors

$$F_\lambda(m_2^\circ,\ldots,m_s^\circ)=\sum_i f_{1i}\otimes\ldots\otimes f_{si}$$

where all $f_{li}\in Hom(\mathbb{F}_q,\mathbb{F}_p)$. If R is some finite subset of $\mathbb{Q}^+(p)$, $r_1,\ldots,r_s\in R$, we use the above expression to define the element $D_\lambda(r_1,0,r_2,m_2^\circ,\ldots,r_s,m_s^\circ)$ of $\mathcal{L}_{R,N}$ by the following equality:

$$D_\lambda(r_1,0,r_2,m_2^\circ,\ldots,r_s,m_s^\circ)=\sum_i[\ldots[D_{r_1,f_{1i}},D_{r_2,f_{2i}}],\ldots,D_{r_s,f_{si}}]$$

It is clear that this element does not depend on the above chosen expression of $F_\lambda(m_2^\circ,\ldots,m_s^\circ)$ as a sum of elementary tensors.

4.3. The constants $\hat{\eta}(r_1, n_1, ..., r_s, n_s)$.

For a natural number $s < p$ and $r_1, ..., r_s \in \mathbb{Q}^+(p)$ we have the structural constants $\eta(r_1, ..., r_s) \in \mathbb{F}_p$ from n.3.1. We set:

$$\hat{\eta}(r_1, ..., r_s) := \eta(r_s, ..., r_1)$$

Consider the collection $(r_1, m_1, r_2, m_2, ..., r_s, m_s)$, where $s < p$, $r_1, ..., r_s \in \mathbb{Q}^+(p)$, $m_1, ..., m_s$ are nonnegative integers. We set

$$\hat{\eta}(r_1, m_1, r_2, m_2, ..., r_s, m_s) = \hat{\eta}(r_1, ..., r_{s_1})\hat{\eta}(r_{s_1+1}, ..., r_{s_2}) ... \ \hat{\eta}(r_{s_{l-1}} + 1, ..., r_{s_l})$$

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

$$\hat{\eta}(r_1, m_1, r_2, m_2, ..., r_s, m_s) = 0$$

otherwise, i.e. if $m_1 \leq m_2 \leq ... \leq m_s$ is not true.

4.4. Definition of a filtration $\{\widetilde{\mathcal{L}}^{(v)}\}_{v>0}$.

Let $R \subset \mathbb{Q}^+(p)$ be a finite subset, $N \geq 1$, $q = p^N$. For any $\gamma_0 \in \mathbb{Q}$, $\gamma_0 > 0$, $\lambda \in \mathbb{F}_q$ we define an element $\mathcal{F}_{R,N}\ (\gamma_0, \lambda) \in \mathcal{L}_{R,N}$ by the equality:

$$\mathcal{F}_{R,N}(\gamma_0, \lambda) =$$

$$= \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R \\ 0 \leqslant m_2, ..., m_s < N \\ r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}} = \gamma_0}} (-1)^{s+1} r_1 \hat{\eta}(r_1, 0, r_2, m_2, ..., r_s, m_s) D_\lambda(r_1, 0, r_2, m_2, ..., r_s, m_s).$$

It is clear from the definition of the constants $\hat{\eta}(r_1, 0, r_2, m_2, ..., r_s, m_s)$ that among all possible presentations of γ_0 in the form

$$\gamma_0 = r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}}$$

only the ordered ones are important.

Let $v_0 \in \mathbb{Q}, v_0 > 0$. We define the ideals $\widetilde{\mathcal{L}}_{R,N}^{(v_0)}$ of the Lie algebra $\widetilde{\mathcal{L}}_{R,N}$ as the ideals generated by all $\mathcal{F}_{R,N}(\gamma_0, \lambda) \bmod C_p(\mathcal{L}_{R,N})$ where $\gamma_0 \geq v_0$ and $\lambda \in \mathbb{F}_q$, $q = p^N$.

It is clear that these ideals give a decreasing filtration in $\widetilde{\mathcal{L}}_{R,N}$. We want to use them to define the "ramification" filtration of the Lie algebra $\widetilde{\mathcal{L}} = \varprojlim \widetilde{\mathcal{L}}_{R,N}$. But a priori it is not clear that for any fixed $v_0 \in \mathbb{Q}$ a system of ideals $\{\widetilde{\mathcal{L}}_{R,N}^{(v_0)}\}$ can be included in a projective system $\{\widetilde{\mathcal{L}}_{R,N}\}$. The following proposition provides us with this property.

Proposition. *For any finite subset $R \subset \mathbb{Q}^+(p)$ and $v_0 \in \mathbb{R}$, $v_0 > 0$ there exists a natural number $N_0(R, v_0)$ such that the connecting morphisms*

$$\widetilde{\mathcal{L}}_{R,N_1} \longrightarrow \widetilde{\mathcal{L}}_{R,N_2}, N_2 | N_1$$

of a projective system $\{\widetilde{\mathcal{L}}_{R,N}\}$ *induce for* $N_2 \geq N(R, v_0)$ *epimorphisms*

$$\widetilde{\mathcal{L}}^{(v_0)}_{R,N_1} \longrightarrow \widetilde{\mathcal{L}}^{(v_0)}_{R,N_2}.$$

The proof of this proposition will be given in n.5 below.

We use this proposition in order to set

$$\widetilde{\mathcal{L}}^{(v_0)} = \varprojlim_{R,N} \widetilde{\mathcal{L}}^{(v_0)}_{R,N}$$

for any $v_0 \in \mathbb{Q}, v_0 > 0$.

5. Proof of proposition n.4.4.

Let R be some finite set in $\mathbb{Q}^+(p)$, $N \geq 1$, $k = \bar{\mathbb{F}}_p$. It is clear that it is sufficient to prove the proposition for ideals $\widetilde{\mathcal{L}}^{(v_0)}_{R,N} \otimes k$ in a projective system $\{\widetilde{\mathcal{L}}_{R,N} \otimes k\}_{R,N}$ of Lie algebras over k.

5.1. Let $q = p^N$.

Lemma. *There exist two* $\mathbb{F}_p$*-bases* $\{\alpha_i\}_{1\leq i\leq N}$ *and* $\{\beta_i\}_{1\leq i\leq N}$ *of* $\mathbb{F}_q$ *such that for any natural number* n *we have*

$$\sum_{1\leq i\leq N} \beta_i^{p^n} \alpha_i = \delta(n, 0),$$

where $\delta(n,0) = 1$ *if* $n \equiv 0 \bmod N$, *and* $\delta(n,0) = 0$ *otherwise.*

Proof. Let $\alpha_0 \in \mathbb{F}_q$ be such that the elements of $\{\alpha_0^{p^i}\}_{0\leq i<N}$ give a (normal) basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. It is easy to see that the basis $\{\alpha_i\}_{1\leq i\leq N}$, where $\alpha_i = \alpha_0^{p^i}, 1 \leq i \leq N$, and its dual basis $\{\beta_i\}_{1\leq i\leq N}$ satisfy the requirements of our lemma.

Let $\{\alpha_i\}_{1\leq i\leq N}$ and $\{\beta_i\}_{1\leq i\leq N}$ be some bases from the above lemma. We can construct a basis $\{f_i\}_{1\leq i\leq N}$ of $Hom(\mathbb{F}_q, \mathbb{F}_p)$ by taking $f_i \in Hom(\mathbb{F}_q, \mathbb{F}_p)$ such that $f_i(\alpha) = Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_i)$ for every $\alpha \in \mathbb{F}_q$. Then for any $r \in R$ and $0 \leq n < N$ we define the elements

$$D_{r,n} = \sum \alpha_i^{p^n} D_{r,f_i} \in \mathcal{L}_{R,N} \otimes k.$$

It is clear that the family $\{D_{r,n}\}_{r\in R, 0\leq n<N}$ can be taken as a system of free generators of the Lie algebra $\mathcal{L}_{R,N} \otimes k$ over k.

Now the tensors $F_\lambda(m_2^\circ, ..., m_s^\circ)$ from n.2 can be written in the following form

$$F_\lambda(m_2^\circ, ..., m_s^\circ) = \sum_{1\leq i_1,...,i_s\leq N} (\alpha_{i_1} \alpha_{i_2}^{p^{m_2^\circ}} ... \alpha_{i_s}^{p^{m_s^\circ}})^{p^n} f_{i_1} \otimes ... \otimes f_{i_s}$$

Therefore,

$$D_\lambda(r_1, 0, r_2, m_2^\circ, ..., r_s, m_s^\circ) = \sum_{0\leq n<N} \lambda^{p^n} [...[D_{r_1,n}, D_{r_2,\widetilde{n+m_2^\circ}}], ..., D_{r_s,\widetilde{n+m_s^\circ}}],$$

where $\widetilde{n+m_l^\circ}$ are residues of $n+m_l^\circ$ from $[0,N)$. Introduce for $\gamma_0 \in \mathbb{Q}, \gamma_0 > 0$ and $0 \le n < N$ the elements of $\mathcal{L}_{R,N} \otimes k$:

$$\mathcal{F}_{R,N}(\gamma_0, n) =$$

$$= \sum_{\substack{1\leqslant s<p \\ r_1,\dots,r_s\in R \\ 0\leqslant m_2,\dots,m_s<N \\ r_1+\frac{r_2}{p^{m_2}}+\dots+\frac{r_s}{p^{m_s}}=\gamma_0}} (-1)^{s+1}\left\{r_1\hat{\eta}(r_1,0,r_2,m_2,\dots,r_s,m_s)[\dots[D_{r_1,n},D_{r_2,\widetilde{n+m_2}}],\dots,D_{r_s,\widetilde{n+m_s}}]\right\}.$$

It follows from the equality

$$\mathcal{F}_{R,N}(\gamma_0,\lambda) = \sum_{0\le n<N} \lambda^{p^n}\mathcal{F}_{R,N}(\gamma_0,n),$$

where $\lambda \in \mathbb{F}_q$, that the ideal $\widetilde{\mathcal{L}}_{R,N}^{(v_0)} \otimes k$ is generated by

$$\mathcal{F}_{R,N}(\gamma_0,n) \operatorname{mod} C_p(\mathcal{L}_{R,N}\otimes k)$$

for all $\gamma_0 \ge v_0$ and $0 \le n < N$.

5.2. In order to write the generators $\mathcal{F}_{R,N}(\gamma_0,n)$ in a more symmetric form we would like to change some notation.

For every integer n such that $0 \le n < N$ we shall use the same symbol when it is considered as its residue modulo N. For every collection $n_1,\dots,n_s$ of integers from $[0,N)$ we define integers n_{ij}, where $1 \le i,j \le s$, by conditions: $n_{ij} \equiv n_i - n_j \bmod N, n_{ij} \in [0,N)$.

We also want to use other notation for the constants $\hat{\eta}(r_1,m_1,r_2,m_2,\dots,r_s,m_s)$, introduced in n.4.3. For every collection $(r_1,n_1,\dots,r_s,n_s)$, where $r_1,\dots,r_s \in R$ and all the n_i are residues modulo N, we set

$$\tilde{\eta}(r_1,n_1,\dots,r_s,n_s) = \hat{\eta}(r_1,n_{11},r_2,n_{12},\dots,r_s,n_{1s})$$

Remark. These constants $\tilde{\eta}(r_1,n_1,\dots,r_s,n_s)$ reflect the idea of "circular" ordering of residues $n_i \operatorname{mod} N$ considered as lying on unit circle via the map:

$$n \operatorname{mod} N \mapsto e^{\frac{2\pi i n}{N}} \in \{z \in \mathbb{C} \mid |z| = 1\}.$$

Now the generators $\mathcal{F}_{R,N}(\gamma_0,n_1)$ can be written in the following form:

$$\mathcal{F}_{R,N}(\gamma_0,n_1) =$$

$$= \sum_{\substack{1\leqslant s<p \\ r_1,\dots,r_s\in R \\ 0\leqslant n_2,\dots,n_s<N \\ r_1+\frac{r_2}{p^{n_{12}}}+\dots+\frac{r_s}{p^{n_{1s}}}=\gamma_0}} (-1)^{s+1} r_1\tilde{\eta}(r_1,n_1,r_2,n_2,\dots,r_s,n_s)[\dots[D_{r_1,n_1},D_{r_2,n_2}],\dots,D_{r_s,n_s}]$$

5.3. We want to investigate the presentations of any given $\gamma \in \mathbb{Q}$ in the form

$$\gamma = r_1 + \frac{r_2}{p^{m_2}} + \dots + \frac{r_s}{p^{m_s}},$$

where $r_1, ..., r_s \in \mathbb{Q}^+(p), m_2, ..., m_s \in \mathbb{N} \cap \{0\}$.

As usual R is a finite subset of $\mathbb{Q}^+(p)$. For any rational $\gamma > 0$ and integer $s \geq 0$ consider the set

$$M_{\gamma,s}(R) =$$

$$= \{(r_1, ..., r_s; m_2, ..., m_s) \in R^s \times \mathbf{Z}^{s-1} | 0 \leq m_2 \leq ... \leq m_s, \gamma = r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_s}{p^{m_s}}\}.$$

The elements of $M_{\gamma,s}(R)$ will be called the decompositions of γ.

Lemma. *$M_{\gamma,s}(R)$ is finite.*

Proof. We use induction on s. For $s = 1$ it is evident. Let $s > 1$ and let the subset $M_{\gamma,s}(r_1, m_2) \subset M_{\gamma,s} = M_{\gamma,s}(R)$ consists of decompositions $(r_1, ..., r_s; m_2, ..., m_s)$ with fixed values of r_1 and m_2. The mapping $(r_1, ..., r_s; m_2, ..., m_s) \mapsto (r_2, ..., r_s; m_3 - m_2, ..., m_s - m_2)$ defines a one-to-one correspondence

$$M_{\gamma,s}(r_1, m_2) \longrightarrow M_{(\gamma - r_1)p^{m_2}, s-1}.$$

R is finite, hence there exists a natural number N_0 such that for every $m_2 > N_0$, $M_{(\gamma - r_1)p^{m_2}, s-1} = \emptyset$. Therefore,

$$M_{\gamma,s} = \cup_{\substack{r_1 \in R \\ m_2 \leq N_0}} M_{\gamma,s}(r_1, m_2)$$

is a finite union of finite sets. The Lemma is proved.

It follows now that the set $M_\gamma(R) = \cup_{1 \leq s < p} M_{\gamma,s}(r)$ of all presentations of γ in the form $r_1 + r_2/p^{m_2} + ... + r_s/p^{m_s}$, where $s < p, r_1, ..., r_s \in R$ and $0 \leq m_2 \leq ... \leq m_s$ is finite.

5.3.2. Now we fix a rational number $v_0 > 0$ and a finite set $R \subset \mathbb{Q}^+(p)$. Let $\gamma \in \mathbb{Q}$, $\gamma > 0$.

Definition.

$$N(R, \gamma) = max\{m_s \mid (r_1, ..., r_s; m_2, ..., m_s) \in M_\gamma(R)\}.$$

Definition. A decomposition $(r_1, ..., r_s; m_2, ..., m_s) \in M_\gamma(R)$ is (v_0, R)-bad if $\gamma \geq v_0$ and for all $1 \leq t \leq s$ and numbers

$$\gamma'_t = r_1 + \frac{r_2}{p^{m_2}} + ... + \frac{r_{s-t}}{p^{m_{s-t}}}$$

the following implication is true:

if $\gamma'_t \geq v_0$ then $N(R, \gamma'_t) \geq m_{s-t+1}$, i.e. there exists a decomposition

$$(r'_1, ..., r'_{s'}; n_2, ..., n_{s'}) \in M_{\gamma'_t}(R)$$

such that $n'_{s'} \geq m_{s-t+1}$ (by definition $m_1 = 1$).

The following properties are the immediate consequences of this definition:

a) A decomposition $\gamma = r_1$, where $r_1 \in R$, $r_1 \geq v_0$, is (v_0, R)-bad;

b) If $(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$ and $\gamma-r_s/p^{n_s}<v_0$ then this decomposition of γ is (v_0,R)-bad;

c) If $(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$ is (v_0,R)-bad and $\gamma_1'=\gamma-r_s/p^{m_s}\geq v_0$ then $(r_1,...,r_{s-1};m_2,...,m_{s-1})\in M_{\gamma_1'}(R)$ is also (v_0,R)-bad ;

d) We obtain from b) and c) that if $\gamma\geq v_0$ and $(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$ is not (v_0,R)-bad then there exists the unique index $s_1<s$ such that the decompositions $(r_1,...,r_{s-1};m_2,...,m_{s-1})\in M_{\gamma_1'}(R)$,...,$(r_1,...,r_{s_1+1};m_2,...,m_{s_1+1})\in M_{\gamma'_{s-s_1+1}}(R)$ are not (v_0,R)-bad and $(r_1,...,r_{s_1};m_2,...,m_{s_1})\in M_{\gamma'_{s-s_1}}(R)$ is (v_0,R)-bad. So, $\gamma_{s-s_1}\geq v_0$ and $N(R,\gamma_{s-s_1})<m_{s_1+1}\leq...\leq m_s$.

Definition. A rational number γ will be called (v_0,R)-bad if there exists a (v_0,R)-bad decomposition $(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$.

Definition. For any natural number N we set

$$M_\gamma(R,N)=\{(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)|m_s<N\}$$

We obtain easily from d):

e) For any given rational number γ_0 and natural number N there exists a finite set J, (v_0,R)-bad numbers $\gamma^{(\alpha)}$, and collections

$$\bar{r}^{(\alpha)}=(r_1^{(\alpha)},...,r_{t_\alpha}^{(\alpha)};m_1^{(\alpha)},...,m_{t_\alpha}^{(\alpha)}),$$

where $\alpha\in J,t_\alpha<p,r_1^{(\alpha)},...,r_{t_\alpha}^{(\alpha)}\in R$, and $0\leq m_1^{(\alpha)}\leq...\leq m_{t_\alpha}^{(\alpha)}$ are integers. For these given data we have:

e_1) $N(R,\gamma^{(\alpha)})<m_1^{(\alpha)}$ for any $\alpha\in J$;

e_2) If for $\alpha\in J$, M_α is the set of all decompositions of the form

$$(r_1,...,r_{s_1},r_1^{(\alpha)},...,r_{t_\alpha}^{(\alpha)};m_2,...,m_{s_1},m_1^{(\alpha)},...,m_{t_\alpha}^{(\alpha)}),$$

where $(r_1,...,r_{s_1};m_2,...,m_{s_1})\in M_{\gamma^{(\alpha)}}(R)$ and $s_1+t_\alpha<p$, then

$$M_\alpha\subset M_{\gamma_0}(R,N);$$

e_3) For any $\alpha_1,\alpha_2\in J,\alpha_1\neq\alpha_2$ we have

$$M_{\alpha_1}\cap M_{\alpha_2}=\emptyset;$$

e_4) $\bigcup_{\alpha\in J}M_\alpha=M_{\gamma_0}(R,N)$.

5.3.3.Lemma. *For any finite subset $R\subset\mathbb{Q}^+(p)$ and a rational number $v_0>0$ the set of all (v_0,R)-bad numbers is finite.*

Proof. By n.5.3.1 it is sufficient to prove the finiteness of the set of all (v_0,R)-bad decompositions.

For any decomposition $\pi=(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$ we define

$$m_0(\pi)=max\{t|\gamma_t'\geq v_0\}$$

if this set is not empty and $m_0(\pi)=0$ otherwise, where numbers γ_t' are taken from the definition of a (v_0,R)-bad decomposition.

Now we take any (v_0,R)-bad decomposition $\pi=(r_1,...,r_s;m_2,...,m_s)\in M_\gamma(R)$ and use an induction on $m_0(\pi)$.

If $m_0(\pi)=0$ then

$$\gamma_1'=\gamma-\frac{r_s}{p^{m_s}}<v_0$$

Lemma. *There exists $\delta = \delta(R, v_0) > 0$ such that*

$$\delta = min\{X = v_0 - \left(\frac{r_1}{p^{m_1}} + ... + \frac{r_l}{p^{m_l}}\right) | l < p, r_1, ..., r_l \in R, m_1, ..., m_s \geq 0, X > 0\}$$

Proof. It is obvious.

We have $r_s/p^{m_s} \geq \delta$ from this lemma, so m_s can only run through a finite set of values. So there exists only a finite number of (v_0, R)-bad decompositions π with $m_0(\pi) = 0$.

Now let $\pi = (r_1, ..., r_s; m_2, ..., m_s)$ be a (v_0, R)-bad decomposition and suppose that our proposition is proved for all (v_0, R)-bad decompositions π' with $m_0(\pi') < m_0^*$, where $m_0^* = m_0(\pi) \geq 1$. By property 5.3.2c), $\pi_1 = (r_1, ..., r_{s-1}; m_2, ..., m_{s-1})$ is (v_0, R)-bad. By the inductive assumption, such decompositions create only a finite set and we can take

$$N^* = max\{N(\gamma', R) | \text{there exists } (v_0, R)\text{-bad } \pi_1 \in M_{\gamma'}(R) \text{ such that } m_0(\pi_1) < m_0^*\}$$

We have $m_s \leq N^*$ because π is (v_0, R)-bad. Again, there is only a finite number of decompositions $(r_1, ..., r_s; m_2, ..., m_s)$ such that $s < p$ and $m_s \leq N^*$. The proposition is proved.

5.3.4. Let

$$N_0(R, v_0) = max\{N(R, \gamma) \mid \gamma \text{ is } (v_0, R)\text{-bad } \} + 1.$$

Lemma. *Let $N \geq N_0(R, v_0)$. Then an ideal $\widetilde{\mathcal{L}}_{R,N}^{(v_0)} \otimes k$ is generated by elements $\mathcal{F}_{R,N}(\gamma, n) \mod C_p(\mathcal{L}_{R,N} \otimes k)$, where $0 \leq n < N$ and γ is (v_0, R)-bad.*

Proof. As was shown in 5.1, $\widetilde{\mathcal{L}}_{R,N}^{(v_0)} \otimes k$ is generated by elements

$$\mathcal{F}_{R,N}(\gamma_0, n) =$$

$$= \sum_{\pi \in M_{\gamma_0}(R,N)} r_1(-1)^{s+1}\hat{\eta}(r_1, 0, r_2, m_2, ..., r_s, m_s)[...[D_{r_1,n}, D_{r_2,\widetilde{n+m_2}}], ..., D_{r_s,\widetilde{n+m_s}}]$$

where $\gamma_0 \geq v_0, 0 \leq n < N, \pi = (r_1, ..., r_s; m_2, ..., m_s)$ and, for $2 \leq i \leq s$, $\widetilde{n + m_i}$ are the representatives of $(n + m_i) \bmod N$ in $[0, N)$.

Now we apply property 5.3.2e). From the definition of the constants $\hat{\eta}$ (c.f. n.4.3) and $\tilde{\eta}$ (c.f. n.5.2), for any decomposition

$$(r_1, ..., r_{s_1}, r_1^{(\alpha)}, ..., r_{t_\alpha}^{(\alpha)}; m_2, ..., m_{s_1}, m_1^{(\alpha)}, ..., m_{t_\alpha}^{(\alpha)}) \in M_\alpha$$

we have

$$\hat{\eta}(r_1, 0, r_2, m_2, ..., r_{s_1}, m_{s_1}, r_1^{(\alpha)}, m_1^{(\alpha)}, ..., r_{t_\alpha}^{(\alpha)}, m_{t_\alpha}^{(\alpha)}) =$$

$$\hat{\eta}(r_1, 0, r_2, m_2, ..., r_{s_1}, m_{s_1})\tilde{\eta}(r_1^{(\alpha)}, m_1^{(\alpha)}, ..., r_{t_\alpha}^{(\alpha)}, m_{t_\alpha}^{(\alpha)})$$

Then the decomposition $\bigcap_{\alpha\in J} M_\alpha = M_{\gamma_0}(R,N)$ gives the following equality:

$$\mathcal{F}_{R,N}(\gamma_0,n) =$$

$$\sum_{\substack{\alpha\in J\\ \pi\in M_\alpha}} (-1)^{s_1+t_\alpha+1} r_1\hat{\eta}(r_1,0,r_2,m_2,\dots,r_{t_\alpha}^{(\alpha)},m_{t_\alpha}^{(\alpha)}) \left[\dots\left[D_{r_1,n},D_{r_2,\widetilde{n+m_2}}\right],\dots,D_{r_{t_\alpha}^{(\alpha)},m_{t_\alpha}^{(\alpha)}}\right] \equiv$$

$$\sum_{\alpha\in J}(-1)^{t_\alpha}\tilde{\eta}(r_1^{(\alpha)},m_1^{(\alpha)},\dots,r_{t_\alpha}^{(\alpha)},m_{t_\alpha}^{(\alpha)}) \left[\dots\left[\mathcal{F}_{R,N}(\gamma^{(\alpha)},n'),D_{r_1^{(\alpha)},\widetilde{n+m_1^{(\alpha)}}}\right],\dots,D_{r_{t_\alpha}^{(\alpha)},\widetilde{n+m_{t_\alpha}^{(\alpha)}}}\right]$$

modulo $C_p(\mathcal{L}_{R,N}\otimes k)$.

This equality proves our lemma.

In order to finish the proof of proposition n.4 we need only state the following:

Lemma. *Let $N_2 \geq N_0(R,v_0), N_2|N_1$ and $\theta_{N_1,N_2} : \widetilde{\mathcal{L}_{R,N_1}} \otimes k \longrightarrow \widetilde{\mathcal{L}_{R,N_2}} \otimes k$ be connecting morphisms of a projective system $\{\widetilde{\mathcal{L}_{R,N}} \otimes k\}$. If γ_0 is (v_0,R)-bad and $0 \leq n < N_1$ then*

$$\theta_{N_1,N_2}(\mathcal{F}_{R,N_1}(\gamma_0,n)) \bmod C_p(\mathcal{L}_{R,N_1}\otimes k) = \mathcal{F}_{R,N_2}(\gamma_0,\tilde{n}) \bmod C_p(\mathcal{L}_{R,N_2}\otimes k),$$

where $\tilde{n} \equiv n \bmod N_2$ and $0 \leq \tilde{n} < N_2$.

Proof. This follows from the equality $M_{\gamma_0}(R) = M_{\gamma_0}(R,N)$ for any (v_0,R)-bad number γ_0 and $N \geq N_0(R,v_0)$.

The proposition of n.4 is proved.

6. Some standard facts about ramification filtrations.

Let K be a local complete discrete valuation field with perfect residue field k of characteristic $p > 0$. For a simplicity we suppose k to be algebraically closed. We denote a separable closure of K by K_{sep} and $\Gamma = Gal(K_{sep}/K)$ will be the absolute Galois group of K.

6.1. Definition of a ramification filtration,[Se3],[De].

Let L be a finite Galois extension of K, $\Gamma_{L/K} = Gal(L/K)$, v_L be a valuation of L such that $v_L(\pi) = 1$, where π is any uniformiser of L. For any real number $x \geq 0$ we set

$$\Gamma_{L/K,x} = \{\tau \in \Gamma_{L/K} \mid v_L(\tau\pi - \pi) \geq x+1\}$$

Then all $\Gamma_{L/K,x}$ are normal subgroups of $\Gamma_{L/K}$. Because k is algebraically closed $\Gamma_{L/K,0} = \Gamma_{L/K}$. So we have a ramification filtration of $\Gamma_{L/K}$ in lower numbering.

Let

$$\psi_{L/K}(x) = \int_0^x [\Gamma_{L/K} : \Gamma_{L/K,x}]^{-1} dx$$

be the Herbrandt function. The relation $\Gamma_{L/K,x} = \Gamma_{L/K}^{(v)}$, where $v = \psi_{L/K}(x)$ for $x \geq 0$, gives the ramification filtration $\{\Gamma_{L/K}^{(v)}\}_{v\geq 0}$ of $\Gamma_{L/K}$ in upper numbering.

Now for every tower of Galois extensions $L_1 \supset L_2 \supset K$ the natural epimorphism $\Gamma_{L_1/K} \longrightarrow \Gamma_{L_2/K}$ gives an epimorphism $\Gamma^{(v)}_{L_1/K} \longrightarrow \Gamma^{(v)}_{L_2/K}$ for every $v \geq 0$. Hence it is possible to define a ramification filtration $\{\Gamma^{(v)}_K\}_{v>0}$ of the absolute Galois group Γ_K by the equality:

$$\Gamma^{(v)}_K = \varprojlim_L \Gamma^{(v)}_{L/K}, \text{ for any } v > 0.$$

The ramification filtration of any separable extension of K may be defined in the same way. So we have:

(1) a decreasing filtration $\{\Gamma^{(v)}_K\}_{v\geq 0}$ of normal subgroups in Γ_K, such that $\Gamma^{(0)}_K = \Gamma_K$, $\bigcap_{v>0} \Gamma^{(v)}_K = \{e\}$;

(2) for every separable extension L/K with the Galois group $\Gamma_{L/K}$, a natural morphism $\Gamma_K \longrightarrow \Gamma_{L/K}$ gives an epimorphism $\Gamma^{(v)}_K \longrightarrow \Gamma^{(v)}_{L/K}$ for every $v \geq 0$;

(3) $I = \bigcup_{v>0} \Gamma^{(v)}_K$ is a pro-p-group and $K^I_{sep} = K_{tr}$ is the maximal tamely ramified extension of K.

6.2. Let L/K be arbitrary finite separable extension. A number $v(L/K)$ is called the *largest upper ramification number* of L/K if the following implication is true:

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

The existence of $v(L/K)$ follows from the left-continuty of the ramification filtration.

The above definition of the Herbrandt function was given in the case that L/K is a Galois extension. Deligne, [De], extended this definition to the case of arbitrary finite separable extensions. We have the following properties:

(1) $\phi_{L/K}(x)$ is a piecewise-linear convex function;

(2) if $(a, \phi_{L/K}(a))$ is the last vertex of the graph of $\phi_{L/K}$, then $v(L/K) = \phi_{L/K}(a)$;

(3) if $K \subset L \subset L_1$ is a tower of finite separable extensions then

$$\phi_{L_1/K} = \phi_{L_1/L}\phi_{L/K}$$

(for the Galois extensions c.f.[Se3], for general case c.f.[De]).

6.3.We say that L/K has the unique ramification number y_0, if $(y_0, \phi_{L/K}(y_0))$ is the unique vertex of the graph of $\phi_{L/K}(x)$. In this case:

$$\phi_{L/K}(x) = \begin{cases} x, & \text{for } 0 \leq x \leq y_0 \\ \frac{x-y_0}{[L:K]} + y_0, & \text{for } x \geq y_0 \end{cases}$$

It is clear that here $y_0 = v(L/K)$.

Lemma. *Let* $\mathrm{char} K = p > 0$, $N \in \mathbb{N}$, $q = p^N$ *and* $r^* \in \mathbb{Q}^+(p)$ *be such that* $r^*(q-1) \in \mathbb{N}$. *Then there exists an extension* K' *of* K *such that*

(1) $[K' : K] = q$;

(2) K'/K *has the unique ramification number* r^*.

Proof.

Let $r^* = \frac{m}{q-1}$, where $m \in \mathbb{N}, (m,p) = 1$. Choose some $t \in K$, such that t^{-1} is an uniformiser of K. Consider extensions

$$K \subset K_N \subset K'_N$$

where $K_N = K(t_N), t_N^{q-1} = t$ and $K'_N = K_N(T_N)$, where $T^q - T = t_N^m$. If $\Gamma_N = Gal(K_N/K)$ and $\Gamma' = Gal(K'_N/K)$, then the natural epimorphism $\Gamma' \longrightarrow \Gamma$ has a section $s : \Gamma \longrightarrow \Gamma'$. It is easy to see that the field $K' = K_N'^{s(\Gamma_N)}$ satisfies the conclusion of the lemma.

Remark. We can choose T in a such a way that $K' = K(T^{q-1})$.

From n.6.1.2 we obtain the following properties.

(1) Let $K \subset K_0 \subset K_1 \subset ... \subset K_n = L$ be a tower of finite separable extensions such that K_0/K is tamely ramified (we write $e_0 = [K_0 : K]$) and for any $1 \le t \le n$, K_{t+1}/K_t is the Galois extension with unique ramification number $x_t > 0$. If $x_1 \le x_2 \le ... \le x_n$ then

$$v(K_n/K) = \frac{1}{e_0}\left(x_1 + \frac{x_2 - x_1}{[K_1 : K_0]} + ... + \frac{x_n - x_{n-1}}{[K_{n-1} : K_0]}\right)$$

(2) Let $K \subset L_1 \subset L_2$ be a tower of finite separable extensions, L_1/K has the unique ramification number y_0 and $v(L_2/L_1) = v_1$. Then

$$v(L_2/K) = max\left\{y_0, \frac{v_1 - y_0}{[L : K]} + y_0\right\}$$

6.4. The following example will be useful in n.7 below.

Example. Let $charK = p$ and $t \in K$ be such that t^{-1} is uniformiser of K.

(1) Let $r \in \mathbb{Q}^+(p), N \in \mathbb{N}, q = p^N$, $\alpha \in k\setminus\{0\}$ and $L = K_{tr}(T)$, where $T^p - T = \alpha t^r$. Then $v(L/K) = r$.

(2) Let $A = \sum_{r \in \mathbb{Q}^+(p)} \alpha_r t^r \in K$, where $\alpha_r \in k$ and almost all are equal to 0. If $L_A = K(T)$, where $T^p - T = A$, then

$$v(L_A/K) = max\{r \mid \alpha_r \neq 0\}.$$

(3) We have also a slight generalisation of (2):
let

$$N \ge 1, q = p^N, B = \sum_{\substack{r \in \mathbb{Q}^+(p) \\ 0 \le n < N}} \alpha_{r,n} t^{rp^n},$$

where $\alpha_{r,n} \in k$ and almost all are equal to 0. Then for $L_B = K(T)$, where $T^q - T = B$, we have:

$$v(L_B/K) = max\{r \mid \alpha_{r,n} \neq 0 \text{ for some } 0 \le n < N\}.$$

7. The main theorem.

Let K be a complete local discrete valuation field of characteristic $p > 0$, with residue field $k \simeq \bar{\mathbf{F}}_p$. As before, let $\Gamma = Gal(K_{sep}/K)$ and $\{\Gamma^{(v)}\}_{v>0}$ be the ramification filtration of Γ. If I is the subgroup of higher ramification we set $\widetilde{\Gamma} = \Gamma/I^pC_p(I)$ and denote by $\{\widetilde{\Gamma}^{(v)}\}_{v>0}$ the image of the ramification filtration of Γ in $\widetilde{\Gamma}$. We also fix $t \in K$ such that t^{-1} is uniformiser of K.

Let e_0 be structural element from n.3.1 and let $\eta(r_1, ..., r_s)$, where $1 \leq s < p$, $r_1, ..., r_s \in \mathbb{Q}^+(p)$, be its structural constants.

Let $\mathcal{L}$ be a profree Lie $\mathbf{F}_p$-algebra from n.3.2, $\widetilde{\mathcal{L}} = \mathcal{L}/C_p(\mathcal{L})$ and let A be an f.a.b. related to $\mathcal{L}$. Then the $(p-1)$-diagonal element $e \in G_{\mathcal{L},K_{tr}}(p-1)$, which has the representative element of the form

$$E = 1 + \sum_{\substack{r_1,...,r_s \in \mathbb{Q}^+(p) \\ i_1,...,i_s \in I}} \eta(r_1, ..., r_s) w_{i_1} ... w_{i_s} t^{r_1 + ... + r_s} D_{i_1,r_1} ... D_{i_s,r_s}$$

(c.f. n.3.2), determines a conjugacy class of isomorphisms of the groups $\widetilde{I} = I/I^pC_p(I)$ and $G_{\mathcal{L},\mathbf{F}_p}(p-1)$. We fix one of them by fixing $f \in G_{\mathcal{L},K_{sep}}(p-1)$ such that $f^{(p)} = fe$, (c.f. n.1). We use this isomorphism below for the identification of the groups $\widetilde{I}$ and $G_{\mathcal{L},\mathbf{F}_p}(p-1)$.

Under this assumption we have the one-to-one mapping

$$\widetilde{exp} : \widetilde{\mathcal{L}} \longrightarrow \widetilde{I} = \bigcup_{v>0} \widetilde{\Gamma}^{(v)}.$$

For any positive rational number $v > 0$ we set $\widetilde{\mathcal{L}}(v) = \widetilde{exp}^{-1}(\widetilde{\Gamma}^{(v)})$. Then $\widetilde{\mathcal{L}}(v)$ is the ideal of the Lie algebra $\widetilde{\mathcal{L}}$. So, we have a decreasing filtration of the ideals $\widetilde{\mathcal{L}}(v)$ in $\widetilde{\mathcal{L}}$.

Theorem. *The filtration $\{\widetilde{\mathcal{L}}^{(v)}\}_{v>0}$ of $\widetilde{\mathcal{L}}$, defined in n.4, coincide with the above filtration $\{\widetilde{\mathcal{L}}(v)\}_{v>0}$.*

Proof.

7.1. Characteristic properties.

Let $J \subset \widetilde{\mathcal{L}}$ be any ideal and let A_J be an f.a.b. over $\mathbf{F}_p$ related to the Lie algebra $\widetilde{\mathcal{L}}/J$. It is clear that the quotient morphism $\mathcal{L} \longrightarrow \widetilde{\mathcal{L}}/J$ gives a morphism of f.a.b. objects $A \longrightarrow A_J$. For any field L of characteristic p we also have the surjective homomorphism of groups

$$G_{\mathcal{L},L}(p-1) \longrightarrow G_{\widetilde{\mathcal{L}}/J,L}(p-1).$$

Let e_J be the image of e under the homomorphism

$$G_{\mathcal{L},K_{tr}}(p-1) \longrightarrow G_{\widetilde{\mathcal{L}}/J,K_{tr}}(p-1)$$

and let f_J be the image of f under the homomorphism

$$G_{\mathcal{L},K_{sep}}(p-1) \longrightarrow G_{\widetilde{\mathcal{L}}/J,K_{sep}}(p-1).$$

We have: $f_J^{(p)} = f_J e_J$, f_J determines an identification of the groups $\widetilde{I}/\widetilde{exp}(J)$ and $G_{\widetilde{\mathcal{L}}/J,\mathbb{F}_p}(p-1)$ and this identification agrees in the obvious sense with the above identification of $\widetilde{I}$ and $G_{\mathcal{L},\mathbb{F}_p}(p-1)$ defined by f.

Let $K_{p-1}(e_J)$ be the field of definition of f_J (c.f. n.1). The following proposition follows immediately from the above construction.

7.1.1. Proposition. *For any $v_0 \in \mathbb{Q}, v_0 > 0$, the ideal $\widetilde{\mathcal{L}}(v_0)$ is the minimal element in the set of ideals $J \subset \widetilde{\mathcal{L}}$, such that the largest upper ramification number $v(K_{p-1}(e_J)/K)$ of the extension $K_{p-1}(e_J)/K$ is less than v_0.*

Let R be any finite subset in $\mathbb{Q}^+(p)$, $N \in \mathbb{N}$ and $\mathcal{L}_{R,N}$ be the Lie $\mathbb{F}_p$-algebra from n.4.1. Then $\mathcal{L} = \varprojlim \mathcal{L}_{R,N}$ and for any $v_0 \in \mathbb{Q}, v > 0$, $\mathcal{L}(v_0) = \varprojlim \mathcal{L}_{R,N}(v_0)$, where $\mathcal{L}(v_0)$ is the inverse image of $\widetilde{\mathcal{L}}(v_0)$ under the quotient $\mathcal{L} \longrightarrow \widetilde{\mathcal{L}}$ and $\mathcal{L}_{R,N}(v_0)$ is the image of $\mathcal{L}(v_0)$ under the projection $\mathcal{L} \longrightarrow \mathcal{L}_{R,N}$.

Analogously, we define elements

$$e_{R,N} \in G_{\mathcal{L}_{R,N},K_{tr}}(p-1) \text{ and } f_{R,N} \in G_{\mathcal{L}_{R,N},K_{sep}}(p-1),$$

such that $e = \varprojlim e_{R,N}$ and $f = \varprojlim f_{R,N}$. We know that the field of definition of f is equal to $\widetilde{K} = K_{sep}^{I^p C_p(I)}$. Let $K_{R,N}$ be the field of definition of $f_{R,N}$ (in the notation of n.1.2.3 we have: $\widetilde{K} = K_e(p-1)$ and $K_{R,N} = K_{e_{R,N}}(p-1)$), then $\widetilde{K} = \varinjlim K_{R,N}$.

For the corresponding ideals $\mathcal{L}_{R,N}(v_0)$ of $\mathcal{L}_{R,N}$ we have the same minimal property as in proposition 7.1.

For any $1 \leq s < p$ we denote by $C_{s+1}(\mathcal{L}_{R,N})$ the ideal of $\mathcal{L}_{R,N}$ generated by all commutators of length $\geq s+1$ and set $\mathcal{L}_{R,N,s}(v_0) = \mathcal{L}_{R,N}(v_0) + C_{s+1}(\mathcal{L}_{R,N})$.

We denote by $K_{R,N,s}$ the field of definition of

$$f_{R,N} \in G_{\mathcal{L}_{R,N},K_{sep}}(s) \subset (A_{R,N} \otimes K_{sep}) \bmod J_{s+1},$$

where $A_{R,N}$ is an f.a.b. related to $\mathcal{L}_{R,N}$ and $J_{s+1} = J_{s+1}(A_{R,N}) \otimes K_{sep}$. Obviously, $K_{R,N,s} \subset K_{R,N}$ and $K_{R,N,s}$ is the maximal Galois extension of K inside $K_{R,N}$ having the higher ramification subgroup of class nilpotency s.

For any ideal I such that $C_{s+1}(\mathcal{L}_{R,N}) \subset I \subset \mathcal{L}_{R,N}$ denote by $K_{R,N,s}(I)$ the field of definition of $f_{R,N} \bmod (IA_{R,N} \otimes K_{sep} + J_{s+1})$. As earlier, we have the following proposition:

7.1.2. Proposition. *$\mathcal{L}_{R,N,s}(v_0)$ is the minimal element in the set of ideals I, such that $C_{s+1}(\mathcal{L}_{R,N}) \subset I \subset \mathcal{L}_{R,N}$ and*

$$v(K_{R,N,s}(I)/K) < v_0.$$

7.2. Restatement of the main theorem.

Let R be a fixed finite subset in $\mathbb{Q}^+(p)$. Let $\delta = \delta(R, v_0) > 0$ be the minimum of all positive values of the expression

$$v_0 - \left(\frac{r_1}{p^{m_1}} + \dots + \frac{r_l}{p^{m_l}}\right),$$

where $1 \leq l < p$, $r_1, ..., r_l$ run over R and $m_1, ..., m_l$ run over $\mathbb{N} \cup \{0\}$ (c.f. 5.3.3).

Choose $N(R, v_0) \in \mathbb{N}$ such that for any $N \geq N(R, v_0)$ there exists $r^* = r^*(N) \in \mathbb{Q}^+(p)$ satisfying the following conditions:

(1) $r^*(q-1) \in \mathbb{N}$, where $q = p^N$;

(2) $r^* < v_0$;

(3) $r^* > \frac{q}{q-1-(p-1)p^{N_0}}(v_0 - \delta)$, where $N_0 = N_0(R, v_0)$ is the natural number from Prop. 4.4.

Now proposition 7.1.2 shows that the following proposition implies our theorem.

Proposition. *For any $N \geq N(R, v_0), 1 \leq s < p$, and ideal I such that*

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

we have:

$$v(K_{R,N,s}(I)/K) < v_0 \quad \Leftrightarrow \quad \widetilde{\mathcal{L}}_{R,N}^{(v_0)} \bmod C_{s+1}(\mathcal{L}_{R,N}) \subset I \bmod C_{s+1}(\mathcal{L}_{R,N}).$$

Remark.

Until the end of n.7 we use the following more simple new notation:

C_s for the ideal $C_s(\mathcal{L}_{R,N})$ of commutators of length $\geq s$ in $\mathcal{L}_{R,N}, 1 \leq s \leq p$;

A for an f.a.b. $A_{\mathcal{L}_{R,N}}$ over $\mathbb{F}_p$ related to $\mathcal{L}_{R,N}$;

A_L for an f.a.b. $A_{\mathcal{L}_{R,N}} \otimes L$, where L is a field, $char L = p$;

A_{sep} for $A_{\mathcal{L}_{R,N}, K_{sep}}$;

J_s for $J_s(A_{\mathcal{L}_{R,N}, K_{sep}}), 1 \leq s \leq p$;

$J_s(O_{sep})$ for the O_{sep}-submodule $J_s(A_{\mathcal{L}_{R,N}}) \otimes O_{sep}$ in $A_{\mathcal{L}_{R,N}, K_{sep}}$, where $1 \leq s \leq p$ and O_{sep} is the valuation ring of K_{sep};

J_s for $J_s(A_{\mathcal{L}_{R,N}, K_{sep}}), 1 \leq s \leq p$;

K_s for the field $K_{R,N,s}$ of definition of $f_{R,N} \bmod J_{s+1}$, $1 \leq s < p$, c.f. n.7.1;

$\mathcal{L}_s(v_0)$ for the ideal $\mathcal{L}_{R,N,s}(v_0)$ from n.7.1;

$K_s(v_0)$ for the field $K_{R,N,s}(\mathcal{L}_{R,N,s}(v_0))$.

7.3. Some identities.

7.3.1. Let $\{D_{r,n} \mid r \in R, 0 \leq n < N\}$ be the system of generators of the Lie k-algebra $\mathcal{L}_{R,N} \otimes k$, which was introduced in 5.1. It is clear that the representative $E \in A_{K_{tr}}$ of $e_{R,N} \in G_{\mathcal{L}_{R,N}, K_{tr}}(p-1)$ can be written in the form

$$E = 1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R}} \eta(r_1, ..., r_s) t^{r_1 + ... + r_s} D_{r_1,0} ... D_{r_s,0}.$$

Let $\mathcal{F}$ be the representative of $f_{R,N}$, then we have:

$$\mathcal{F}^{(p)} \equiv \mathcal{F} E \bmod J_p.$$

7.3.2. Let $E_N = E E^{(p)} ... E^{(p^{N-1})}$. Then

$$E_N \equiv 1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R \\ 0 \leqslant n_1, ..., n_s < N}} \eta(r_1, n_1, ..., r_s, n_s) t^{r_1 p^{n_1} + ... + r_s p^{n_s}} D_{r_1, n_1} ... D_{r_s, n_s} \bmod J_p,$$

where the constants $\eta(r_1, n_1, ..., r_s, n_s)$ are defined as follows:

$$\eta(r_1, n_1, ..., r_s, n_s) = \eta(r_1, ..., r_{s_1})\eta(r_{s_1+1}, ..., r_{s_2})...\eta(r_{s_{l-1}+1}, ..., r_{s_l}),$$

if $n_1 = ... = n_{s_1} < n_{s_1+1} = ... = n_{s_2} < ... < n_{s_{l-1}+1} = ... = n_{s_l}$, where $1 \leq s_1 < s_2 < ... < s_l = s$ and

$$\eta(r_1, n_1, ..., r_s, n_s) = 0,$$

otherwise.

Remark. The constants $\eta(r_1, n_1, ..., r_s, n_s)$ are obtained from the constants $\eta(r_1, ..., r_s)$ in the same way, as the constants $\hat{\eta}(r_1, n_1, ..., r_s, n_s)$ were obtained from the constants $\hat{\eta}(r_1, ..., r_s) = \eta(r_s, ..., r_1)$ in n.4.3.

For $q = p^N$ and the above element E_N we have the following equivalence:

$$\mathcal{F}^{(q)} \equiv \mathcal{F}E_N \operatorname{mod} J_p.$$

7.3.3. Let $\mathcal{F}^* = \mathcal{F}^{(p)}$, then $\mathcal{F}^{(q)} \equiv \mathcal{F}^* E^{(p)} ... E^{(p^{N-1})} \operatorname{mod} J_p$, i.e.

$$\mathcal{F}^{(q)} \equiv \mathcal{F}^*(1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R \\ 0 < n_1, ..., n_s < N}} \eta(r_1, n_1, ..., r_s, n_s) t^{r_1 p^{n_1} + ... + r_s p^{n_s}} D_{r_1, n_1} ... D_{r_s, n_s}) \operatorname{mod} J_p.$$

7.3.4. Let

$$E_0 = E - 1 = \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R}} \eta(r_1, ..., r_s) t^{r_1 + ... + r_s} D_{r_1, 0} ... D_{r_s, 0}.$$

From the equivalence

$$\mathcal{F}^{(p)} - \mathcal{F} \equiv \mathcal{F}E_0 \operatorname{mod} J_p,$$

we obtain

$$\mathcal{F}^{(q)} - \mathcal{F} \equiv \sum_{0 \leq n < N} (\mathcal{F}E_0)^{(p^n)} \operatorname{mod} J_p.$$

7.4. The field K'.

Let $N \geq N(R, v_0), q = p^N$ and $r^* \in \mathbb{Q}^+(p)$ be some number, related to N in the definition of $N(R, v_0)$.

We denote by K' the extension of K, which has the Herbrandt function of the form:

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

(c.f. 6.3).

7.4.1. Lemma. *There exists a* $t_1 \in K'$ *such that*

(1) t_1^{-1} *is a uniformiser of* K';

(2) $t = t_1^q e_1$, *where* $e_1 = \widetilde{exp}\left(-\frac{1}{r^*}t_1^{-r^*(q-1)}\right)$.

Proof. It may be proved by Hensel's lemma from the explicit construction of the field K', c.f. n.6.3.

It is clear that there exists (unique) isomorphism f of the fields K and K', which is the identity on their residue fields and sends t to t_1. The following property of the extension K'/K will be useful later.

7.4.2. Lemma. *Let* L/K *and* L'/K' *be finite extensions such that there exists an isomorphism of fields* $g : L \longrightarrow L'$ *which prolongs* f, *i.e.* $g|_K = f$. *Then* $v(L/K)$ *and* $v(L'/K)$ *are both* $< v_0$ *or* $v(L'/K) < v(L/K)$.

Proof. It follows from the property (2) n.6.3.

7.4.3. The following property is related to a special choice of an r^* and will be useful below.

Let $M_{p-1}(R) =$

$$= \left\{\gamma \in \mathbb{Q} \mid \gamma = \frac{r_1}{p^{m_1}} + \ldots + \frac{r_s}{p^{m_s}}, 1 \leq s < p,\ r_1, \ldots, r_s \in R,\ m_1, \ldots, m_s \in \mathbb{N} \cup \{0\}\right\}$$

and let $O'_{tr} = O_{K'_{tr}}$ be the valuation ring of the field $K'_{tr} = K_{tr}K'$. Then we have the following

Lemma. *If* $\gamma \in M_{p-1}(R), \gamma < v_0$, *then*

$$t_1^{q\gamma - r^*(q-1)} \in t_1^{-r^*(p-1)p^{N_0}} O'_{tr} \subset O'_{tr}.$$

Proof. This follows immediately from the condition (3) of 7.2.

7.5. Some identities.

7.5.1. Let $1 \leq s < p$, $r_1, \ldots, r_s \in R$, $0 \leq n_1, \ldots, n_s < N$. We use the constants $\eta(r_1, n_1, \ldots, r_s, n_s)$, $\hat{\eta}(r_1, n_1, \ldots, r_s, n_s)$ and $\tilde{\eta}(r_1, n_1, \ldots, r_s, n_s)$, which were defined in n.7.3.2, n.4.3, n.5.2, respectively.

We use the agreement about indices from n.5.2, i.e. for any natural numbers $n_1, \ldots, n_s$ we denote by n_{ij}, where $1 \leq i, j \leq s$, the reduced residue of $n_i - n_j$ modulo N, i.e. n_{ij} is uniquely defined by the conditions:

$$n_{ij} \equiv n_i - n_j \bmod N,\ 0 \leq n_{ij} < N.$$

We have:

$$\tilde{\eta}(r_1, n_1, \ldots, r_s, n_s) = \eta(r_s, \ldots, r_1), \text{ if } n_1 = \ldots = n_s;$$

and

$$\tilde{\eta}(r_1, n_1, \ldots, r_s, n_s) = \hat{\eta}(r_1, n_{11}, \ldots, r_s, n_{1s}).$$

We introduce new constants $\eta^*(r_1, n_1^*, \ldots, r_s, n_s^*)$, where $1 \leq s < p$, $r_1, \ldots, r_s \in R$, $n_1^*, \ldots, n_s^* \in (0, N]$.

Definition.

$$\eta^*(r_1,n_1^*,...,r_s,n_s^*)=\hat{\eta}(r_1,...,r_{s_1})\hat{\eta}(r_{s_1+1},...,r_{s_2})...\hat{\eta}(r_{s_{l-1}+1},...,r_{s_l}),$$

if $n_1^*=...=n_{s_1}^*>n_{s_1+1}^*=...=n_{s_2}^*>...>n_{s_{l-1}+1}^*=...=n_{s_l}^*$, where $1\leq s_1<s_2<...<s_l=s$ (we recall, that $\hat{\eta}(r_1,...,r_{s_1})=\eta(r_{s_1},...,r_1)$, c.f. n.4.3), and

$$\eta^*(r_1,n_1^*,...,r_s,n_s^*)=0$$

otherwise, i.e. if $n_1^*\geq...\geq n_s^*$ is not true.

We have:

$$\tilde{\eta}(r_1,n_1,...,r_s,n_s)=\eta^*(r_1,n_{11}^*,...,r_s,n_{s1}^*)=\hat{\eta}(r_1,N-n_{11}^*,r_2,N-n_{21}^*,...,r_s,N-n_{s1}^*),$$

where n_{ij}^* are the residues modulo N of n_i-n_j from $(0,N]$ (it is sufficient to remark that for any i,j we have $n_{ij}^*=N-n_{ji}$).

7.5.2. For the constants $\eta(r_1,n_1,...,r_s,n_s)$ we have the following analogue of lemma 3.1.

Lemma. *If s_1,s_2 are natural numbers such that $s=s_1+s_2<p$, then*

$$\eta(r_1,n_1,...r_{s_1},n_{s_1})\eta(r_{s_1+1},n_{s_1+1},...,r_{s_2},n_{s_2})=\sum_{\sigma\in P_{s_1,s_2}}\eta(r_{\sigma(1)},n_{\sigma(1)},...,r_{\sigma(s_2)},n_{\sigma(s_2)}),$$

where P_{s_1,s_2} is the subset of permutations of order s_2 such that $\sigma(i)<\sigma(j)$,where $1\leq i<j\leq s_1$ or $s_1+1\leq i<j\leq s_2$.

Proof. This follows from the fact that

$$1+\sum_{\substack{1\leqslant s<p\\ r_1,...,r_s\in R\\ 0\leqslant n_1,...,n_s<N}}\eta(r_1,n_1,...,r_s,n_s)D_{r_1,n_1}...D_{r_s,n_s}$$

is the representative of a $(p-1)$-diagonal element.

Remark. The meaning of the right side of the above formula is very simple:

the collections of variables are numerated by all inclusions of the first set of indices $\{1,...,s_1\}$ into the second set $\{s_1+1,...,s_2\}$, which conserve the natural orderings of these sets.

Remark. By the same reasoning the analogous statement is true for the constants $\hat{\eta}(r_1,n_1,...,r_s,n_s)$ and $\eta^*(r_1,n_1^*,...,r_s,n_s^*)$.

7.5.3. Let s be any natural number.

Definition. A subset Φ_s of "connected" permutations of order s consists of all one-to-one mappings $\sigma:\{1,...,s\}\longrightarrow\{1,...,s\}$ such that for any $1\leq s_1\leq s$ the set $\{\sigma(1),...,\sigma(s_1)\}$ consists of s_1 sequential integers.

Lemma. *For any indeterminates $D_1, ..., D_s$ we have:*

$$[...[D_1, D_2], ..., D_s] = \sum_{\sigma \in \Phi_s} (-1)^{\sigma^{-1}(1)-1} D_{\sigma^{-1}(1)} D_{\sigma^{-1}(2)} ... D_{\sigma^{-1}(s)}.$$

Proof. It may be proved by some combinatorial arguments.

7.5.4. Let $1 \le s < p$, $r_1, ..., r_s \in R$, $0 \le n_1, ..., n_s < N$.

Definition. For $1 \le t \le s$ we set

$$B_t(r_1, n_1, ..., r_s, n_s) = \sum_{\substack{\sigma \in \Phi_s \\ \sigma(1)=t}} \tilde{\eta}(r_{\sigma(1)}, n_{\sigma(1)}, ..., r_{\sigma(s)}, n_{\sigma(s)}).$$

Example.

$$B_1(r_1, n_1) = \tilde{\eta}(r_1, n_1) = 1,$$

$$B_2(r_1, n_1, r_2, n_2, r_3, n_3) = \tilde{\eta}(r_2, n_2, r_1, n_1, r_3, n_3) + \tilde{\eta}(r_2, n_2, r_3, n_3, r_1, n_1),$$

$$B_1(r_1, n_1, ..., r_s, n_s) = \tilde{\eta}(r_1, n_1, ..., r_s, n_s),$$

$$B_s(r_1, n_1, ..., r_s, n_s) = \tilde{\eta}(r_s, n_s, ..., r_1, n_1).$$

Lemma. *For any $\gamma_0 \in \mathbb{Q}$, $\gamma_0 > 0$ and natural number n^* we have:*

$$\sum_{\substack{r_1, ..., r_s \in R \\ 0 \leqslant n_2, ..., n_s < N \\ n_1 = n^* \\ r_1 + \frac{r_2}{p^{n_{12}}} + ... + \frac{r_s}{p^{n_{1s}}} = \gamma}} r_1 \tilde{\eta}(r_1, n_1, ..., r_s, n_s)[...[D_{r_1,n_1}, D_{r_2,n_2}], ..., D_{r_s,n_s}] =$$

$$= \sum_{1 \le t \le s} \sum_{\substack{r_1, ..., r_s \in R \\ 0 \leqslant n_1, ..., n_{t-1}, n_{t+1}, ..., n_s < N \\ n_t = n^* \\ \frac{r_1}{p^{n_{t1}}} + ... + \frac{r_s}{p^{n_{ts}}} = \gamma}} (-1)^{t+1} r_t B_t(r_1, n_1, ..., r_s, n_s) D_{r_1,n_1} ... D_{r_s,n_s}.$$

Proof. This follows from lemma 7.5.3.

7.5.5.

Lemma.

$$B_t(r_1, n_1, ..., r_l, n_l) + \delta(n_t, n_{t+1}) B_{t+1}(r_1, n_1, ..., r_l, n_l) =$$

$$= \eta^*(r_t, n_{tt}^*, ..., r_1, n_{1t}^*) \eta^*(r_{t+1}, n_{t+1,t}^*, ..., r_l, n_{l,t}^*),$$

where

$$\delta(n_t, n_{t+1}) = \begin{cases} 1, & \text{if } n_t = n_{t+1}, \\ 0, & \text{otherwise}. \end{cases}$$

Proof. Let $n_t \neq n_{t+1}$, then

$$B_t(r_1, n_1, ..., r_l, n_l) = \sum_{\substack{\sigma \in \Phi_l \\ \sigma(1)=t}} \tilde{\eta}(r_t, n_t, ..., r_{\sigma(i)}, n_{\sigma(i)}, ..., r_{\sigma(l)}, n_{\sigma(l)}) =$$

$$= \sum_{\substack{\sigma \in \Phi_l \\ \sigma(1)=t}} \eta^*(r_t, n^*_{tt}, ..., r_{\sigma(i)}, n^*_{\sigma(i),t}, ...) + \sum_{\substack{\sigma \in \Phi_l \\ \sigma(1)=t}} \eta^*(r_{t+1}, n^*_{t+1,t}, ..., r_{\sigma(i)}, n^*_{\sigma(i),t}, ...) =$$

(all summands of the second sum are equal to 0, because $n^*_{t+1,t} < n^*_{t,t} = 0$)

$$= \eta^*(r_t, n^*_{tt}, ..., r_1, n^*_{1t})\eta^*(r_{t+1}, n^*_{t+1,t}, ..., r_l, n^*_{l,t})$$

by the lemma and remarks of n.7.4.2.

The same arguments gives the proof in the case $n_t = n_{t+1}$.

7.5.6.

Definition.

$$B^*_t(r_1, n_1, ..., r_s, n_s) = \begin{cases} B_t(r_1, n_1, ..., r_s, n_s), & \text{for } n_t \geq ... \geq n_s, \\ 0, & \text{otherwise.} \end{cases}$$

Example.

$$B^*_1(r_1, n_1, ..., r_s, n_s) = \eta(r_s, n_s, ..., r_1, n_1),$$

$$B^*_s(r_1, n_1, ..., r_s, n_s) = B_s(r_1, n_1, ..., r_s, n_s),$$

$$B^*_t(r_1, n_1, ..., r_{s-1}, n_{s-1}, r_s, 0) = B_t(r_1, n_1, ..., r_{s-1}, n_{s-1}, r_s, 0).$$

Remark.

$$B^*_t(r_1, n_1, ..., r_s, n_s) = B_t(r_1, n_1, ..., r_s, n_s),$$

if $n_t \geqslant n_s$.

Lemma. *If* $n_{t+1} \leq n_t$, $l \geq t+1$, *then*

$$B^*_t(r_1, n_1, ..., r_l, n_l) + \delta(n_t, n_{t+1})B^*_{t+1}(r_1, n_1, ..., r_l, n_l) =$$

$$= \tilde{\eta}(r_t, n_t, ..., r_1, n_1)B^*_1(r_{t+1}, n_{t+1}, ..., r_l, n_l).$$

Proof. If $n_{t+1} \geq ... \geq n_l$ is not true, then the both sides are equal to 0.

If $n_{t+1} \geq ... \geq n_l$, then for any $t+1 \leq u \leq l$ we have $n_{t,u} = n_{t,t+1} + n_{t+1,u}$ or (equivalently) $n^*_{u,t} = (n^*_{t+1,t} - N) + n^*_{u,t+1}$.

Therefore,

$$\eta^*(n^*_{t+1,t+1}, n^*_{t+2,t+1}, ..., n^*_{l,t+1}) = \eta^*(n^*_{t+1,t}, n^*_{t+2,t}, ..., n^*_{l,t}).$$

Now our lemma follows from lemma 7.5.5.

7.5.7.

Proposition. *We have the following identity:*

$$B_t^*(r_1, n_{1s}, ..., r_s, n_{ss}) - B_t^*(r_1, n_{1s}, ..., r_{s-1}, n_{s-1,s})\eta(r_s, n_{ss}) +$$

$$+ B_t^*(r_1, n_{1s}, ..., r_{s-2}, n_{s-2,s})\eta(r_{s-1}, n_{s-1,s}, r_s, n_{ss}) - ... +$$

$$+(-1)^{s-t+1} B_t^*(r_1, n_{1s}, ..., r_t, n_{ts})\eta(r_{s+1}, n_{t+1,s}, ..., r_s, n_s) +$$

$$+(-1)^{s-t}\tilde{\eta}(r_s, n_s, ..., r_1, n_1)|_{n_t = ... = n_s} = 0,$$

where by definition $\eta(r_s, n_s, ..., r_1, n_1)|_{n_t=...=n_s}$ *is equal to* $\eta(r_s, n_s, ..., r_1, n_1)$, *if* $n_t = ... = n_s$, *and is equal to 0, otherwise.*

Proof.

1st step. Let $t = 1$. Then in evident notation we must prove:

$$\eta(s, ..., 1) - \eta(s-1, ..., 1)\eta(s) + \eta(s-2, ..., 1)\eta(s, s-1) + ...$$

$$+(-1)^s\eta(1)\eta(2, ..., s) = (-1)^s\tilde{\eta}(s, ..., 1)|_{n_1=...=n_s}$$

It follows from the lemma and remark of n.7.4.2 that the left-hand side of the above equality is equal to

$$(-1)^s\eta(1, ..., s) = (-1)^s\eta(r_1, n_{1s}, ..., r_s, n_{ss}).$$

It follows from definition of the constants η (c.f. n.7.3.2), that

$$\eta(r_1, n_{1s}, ..., r_s, n_{ss}) \neq 0 \;\Leftrightarrow\; n_1 = ... = n_s$$

and, if $n_1 = ... = n_s$, then

$$\eta(r_1, n_{1s}, ..., r_s, n_{ss}) = \tilde{\eta}(r_s, n_s, ..., r_1, n_1).$$

2nd step.

Let $n_{ts} \neq n_{t+1,s}$. If $n_{ts} < n_{t+1,s}$, there is nothing to prove.

If $n_{ts} > n_{t+1,s}$, then we can apply lemma n. 7.5.6 :

$$B_t^*(1, ..., l) = \tilde{\eta}(t, ..., 1)B_1^*(t+1, ..., l).$$

Therefore the left side of the identity is equal to

$$\tilde{\eta}(t, ..., 1)\left[B_1^*(t+1, ..., s) - B_1^*(t+1, ..., s-1)\eta(s) + ... + (-1)^{s-t+1}\eta(t+1, ..., s)\right] = 0,$$

by the first step.

3rd step.

Let $n_t = n_{t+1}$. Then we can assume, that $n_t = n_{t+1} = ... = n_{t+l} \neq n_{t+l+1}$. By the 2nd step we have the assertion of our lemma, where t is replaced by $t+l$. Now we can apply lemma of n.7.5.6 and obtain the assertion of our lemma by some induction arguments.

7.6. Consider the extension K' of K from n.7.4. We can assume, that K_{sep} is chosen in such a way, that $K \subset K' \subset K_{sep}$. Then $A_K \subset A_{K'} \subset A_{K_{sep}}$ and we use these inclusions for the identification of $A_{K'_{sep}}$ and $A_{K_{sep}}$.

On the other hand, consider the isomorphism f of the fields K and K' from n.7.4.1. f can be extended to isomorphisms K_{sep} and K'_{sep}, A_K and $A_{K'}$, $A_{K_{sep}}$ and $A_{K'_{sep}}$, respectively. The composition of the last isomorphism $A_{K_{sep}} \longrightarrow A_{K_{sep'}}$ with the above identification of $A_{K_{sep'}}$ and $A_{K_{sep}}$ will be denoted by the same symbol f.

The following facts are the obvious consequences of this definition.

(1) Let

$$E = 1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R}} \eta(r_1, ..., r_s) t^{r_1 + ... + r_s} D_{r_1,0} ... D_{r_s,0} \in A_{K_{tr}}$$

(c.f. n.7.3), then

$$E' = f(E) = 1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R}} \eta(r_1, ..., r_s) t_1^{r_1 + ... + r_s} D_{r_1,0} ... D_{r_s,0} \in A_{K'_{tr}},$$

where $K'_{tr} = K' K_{tr}$.

(2) Consider $\mathcal{F} \in A_{K_{sep}}$ from n.7.3 and set $f(\mathcal{F}) = \mathcal{F}'$, $E'_0 = f(E_0) = E' - 1$. Then

$$\mathcal{F}'^{(p)} \equiv \mathcal{F}' E' \operatorname{mod} J_p,$$

$$\mathcal{F}'^{(q)} \equiv \mathcal{F}'^{*}(1 + \sum_{\substack{1 \leqslant s < p \\ r_1, ..., r_s \in R \\ 0 < n_1, ..., n_s < N}} \eta(r_1, n_1, ..., r_s, n_s) t_1^{r_1 p^{n_1} + ... + r_s p^{n_s}} D_{r_1,n_1} ... D_{r_s,n_s}) \operatorname{mod} J_p,$$

$$\mathcal{F}'^{(q)} - \mathcal{F}' \equiv \sum_{0 \leq n < N} (\mathcal{F}' E'_0)^{(p^n)} \operatorname{mod} J_p.$$

(3) For $1 \leq s < p$ the field of definition of $\mathcal{F}' \operatorname{mod} J_{s+1}$ is equal to $K'_{R,N,s} = f(K_{R,N,s})$. The field of definition of $\mathcal{F}' \operatorname{mod}(\mathcal{L}_s(v_0) A_{sep} + J_{s+1})$ equals to $K'_s(v_0) = f(K_s(v_0))$ - the maximal Galois extension of K' inside $K'_{R,N}$, which has the higher ramification subgroup of class of nilpotency $\leq s$ and upper ramification numbers $< v_0$.

7.7. Inductive assumption.

We use an induction on s^* in order to prove the following statements for $1 \leq s^* < p$. Obviously, our theorem follows from the following statement.

Proposition. *Let* $1 \leqslant s^* < p$. *Then*

(a) $\mathcal{L}_{s^*}(v_0) = \mathcal{L}^{(v_0)}_{R,N} + C_{s^*+1}$;

(b) $K_{s^*}(v_0)K' = K'_{s^*}(v_0)$;

(c) $\mathcal{F} \equiv$

$$\equiv \mathcal{F}'^{(q)} + X(s^*) \bmod \left(\mathcal{L}_{s^*}(v_0)A_{sep} + \sum_{1 \leqslant s \leqslant s^*} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s^*+1} \right),$$

where $X(s^*) \equiv$

$$\equiv \sum_{\substack{1 \leqslant t \leqslant s \leqslant s^* \\ r_1,\dots,r_s \in R \\ 0 \leqslant n_1,\dots,n_s < N}} \mathcal{F}'^{*(p^{n_t})}(-1)^{s+t+1} B^*_t(r_1,n_1,\dots,r_s,n_s) \left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}}+\dots+\frac{r_t}{p^{n_{ts}}}\right)} (e_1^{r_t}-1) \right]^{p^{n_t}} \times$$

$$\times e_1^{r_{t+1}p^{n_{t+1}}} \dots e_1^{r_s p^{n_s}} D_{r_1,n_1} \dots D_{r_s,n_s} (\bmod J_{s^*+1}).$$

(we use the agreement about indices from n.7.5.1);

(d) $A(s^*)_0 =$

$$= \sum_{\substack{1 \leqslant s \leqslant s^* \\ 0 \leqslant n_1,\dots,n_s < N \\ r_1,\dots,r_s \in R}} \sum_{1 \leqslant t \leqslant s} (-1)^{s+t} B_t(r_1,n_1,\dots,r_s,n_s) \left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}}+\dots+\frac{r_t}{p^{n_{ts}}}\right)} (e_1^{r_t}-1) \right]^{p^N} \times$$

$$\times e_1^{r_{t+1}p^{N-n_{t,t+1}}} \dots e_1^{r_s p^{N-n_{ts}}} D_{r_1,n_1} \dots D_{r_s,n_s}$$

is the element of $\mathcal{L}_{s^*}(v_0)A_{sep} + \sum_{1 \leqslant s \leqslant s^*} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s^*+1}$.

7.8. The case $s^* = 1$.

This case is very simple. We take an element $\mathcal{F}$ in the form:

$$\mathcal{F} \equiv 1 + \sum_{\substack{r \in R \\ 0 \leq n < N}} T_{r,n} D_{r,n} \bmod J_2.$$

Then the equivalence (c.f. n.7.3.4)

$$\mathcal{F}^{(q)} - \mathcal{F} \equiv \sum_{0 \leqslant n < N} (\mathcal{F}E_0)^{(p^n)} \equiv \sum_{\substack{0 \leqslant n < N \\ r \in R}} t^{rp^n} D_{r,n} \bmod J_2$$

gives the equations

$$T^q_{r,n} - T_{r,n} = t^{rp^n},$$

where $r \in R, 0 \leq n < N$ and we conclude from n.6.4, that $\mathcal{L}_1(v_0) \otimes k \bmod J_2$ is generated by

$$\{D_{r,n} \mid r \geq v_0,\ 0 \leq n < N\}.$$

But this set is the set of generators of $(\widetilde{\mathcal{L}}_{R,N}^{(v_0)} \otimes k) \operatorname{mod} C_2 \otimes k$, c.f. n.5.1. So,

$$\mathcal{L}_1(v_0) \operatorname{mod} C_2 = \widetilde{\mathcal{L}}_{R,N}^{(v_0)} \operatorname{mod} C_2.$$

We have also

$$E_0 \equiv E_0'^{(q)} + \sum_{r\in R} t_1^{qr}(e_1^r - 1)D_{r,0} \operatorname{mod} J_2,$$

where E_0' was defined in n.7.6. Let $\mathcal{F}' \in A_{K_{sep}}$ be the element from n.7.6, then the identity from n.7.3.4 gives

$$\mathcal{F}^{(q)} - \mathcal{F} \equiv \sum_{0\leqslant n<N} E_0^{(p^n)} \equiv \sum_{0\leqslant n<N} \left[(E_0')^{(p^n)}\right]^{(q)} - X(1) \equiv$$

$$\equiv \left[(\mathcal{F}')^{(q)} - \mathcal{F}'\right]^{(q)} - X(1)(\operatorname{mod} J_2),$$

where

$$X(1) = -\sum_{\substack{0\leqslant n<N\\ r\in R}} [t_1^{qr}(e_1^r - 1)]^{p^n} D_{r,n}.$$

We set

$$\mathcal{F} \equiv \mathcal{F}'^{(q)} + X(1) + Y \operatorname{mod} J_2,$$

where $Y^{(q)} - Y = A(1)$,

$$A(1) = \sum_{0\leqslant n<N} A(1)_0^{(p^n)}$$

and

$$A(1)_0 = \sum_{r\in R} [t_1^{qr}(e_1^r - 1)]^q D_{r,0}.$$

One may check that

$$A(1)_0 \in \mathcal{L}_1(v_0)A_{sep} + t^{-r^*(p-1)}J_1(O_{sep}).$$

Indeed, if $r \geq v_0$, then $D_{r,0} \in \mathcal{L}_1(v_0) \otimes k$, as was shown earlier. If $r < v_0$, then $t_1^{qr-r^*(q-1)} \in t_1^{-r^*(p-1)}O'_{tr}$ (c.f. n.7.4.3), therefore,

$$[t_1^{qr}(e_1^r - 1)]^q D_{r,0} \in t^{-r^*(p-1)}J_1(O_{sep}).$$

Now it is clear, that $Y \in \mathcal{L}_1(v_0)A_{sep} + t^{-r^*(p-1)}J_1(O_{sep})$. Therefore,

$$\mathcal{F} \equiv \mathcal{F}'^{(q)} + X(1) \operatorname{mod} \mathcal{L}_1(v_0)A_{sep} + t^{-r^*(p-1)}J_1(O_{sep}) + J_2.$$

The fact, that $X(1)$ is defined over K', implies the equality $K_1(v_0)K' = K_1'(v_0)$.

7.9. Some calculations.

Let s_0 be such that $1 < s_0 < p$ and assume, that our inductive assumption (Prop. of n.7.7) is valid for all $1 \leq s^* < s_0$.

7.9.1. Proposition. *Let E_0 be the element from n.7.3.4, then*

$$E_0 \in \mathcal{L}_{s_0-1}(v_0)A_{sep} + \sum_{1\leqslant s<s_0} t^{r^*s}J_s(O_{sep}) + J_{s_0}.$$

Proof. We use the following Lemma:

Lemma. *Let $r \in R$, $s_1 \in \mathbb{N}$, $0 \le n < N$ and $r \ge s_1 r^*$. Then*

$$D_{r,n} \in (\mathcal{L}_{s_0-1}(v_0) + C_s) \otimes k,$$

where $s = \min\{s_1+1, s_0\}$.

Proof. By 7.7 (a) $\mathcal{L}_{s_0-1}(v_0) = \mathcal{L}_{R,N}^{(v_0)} + C_{s_0}$, so $\mathcal{L}_{s_0-1}(v_0) \otimes k \bmod C_{s_0} \otimes k$ is generated (as an ideal) by the elements $\mathcal{F}_{R,N}(\gamma, n)$, where $\gamma \ge v_0, 0 \le n < N$ (c.f. n.5). Now we can apply induction on s_1 to show that, if $r \ge s_1 r^*$, then $\mathcal{F}_{R,N}(r,n) \equiv D_{r,n} \bmod C_s \otimes k$, where $s = \min\{s_1+1, s_0\}$. The Lemma is proved.

Now the above Proposition can be proved as follows. The expression for $E_0 \bmod J_{s_0}$ is a linear combination over $\mathbf{F}_p$ of the terms $t^{r_1+\dots+r_l} D_{r_1,0} \dots D_{r_l,0}$, where $1 \le l < s_0$, $r_1, \dots, r_l \in R$. We use induction on l to show that these terms are in $\mathcal{L}_{s_0-1}(v_0)A_{sep} + \sum_{1\le s<s_0} t^{r^*s} J_s(O_{sep})$.

If $l = 1$ and $(s_1+1)r^* > r_1 \ge s_1 r^*$ the above lemma gives

$$D_{r_1,0} \in \mathcal{L}_{s_0-1}(v_0) \otimes k + J_{s_1+1}(O_{sep}) + J_{s_0},$$

therefore,

$$t^{r_1} D_{r_1,0} \in \mathcal{L}_{s_0-1}(v_0)A_{sep} + t^{(s_1+1)r^*} J_{s_1+1}(O_{sep}) + J_{s_0}.$$

Let $l > 1$ and $(s+1)r^* > r_1 + \dots + r_l \ge sr^*$. By the inductive assumption we have:

if $(s_1+1)r^* > r_1 + \dots + r_{l-1} \ge s_1 r^*$, then

$$t^{r_1+\dots+r_{l-1}} D_{r_1,0} \dots D_{r_{l-1},0} \in \mathcal{L}_{s_0-1}(v_0)A_{sep} + t^{(s_1+1)r^*} J_{s_1+1}(O_{sep}) + J_{s_0}.$$

It follows from the above inequalities that $r_l \ge (s - s_1 - 1)r^*$, therefore,

$$t^{r_l} D_{r_l,0} \in \mathcal{L}_{s_0-1}(v_0)A_{sep} + t^{(s-s_1)r^*} J_{s-s_1}(O_{sep}) + J_{s_0},$$

and we obtain

$$t^{r_1+\dots+r_l} D_{r_1,0} \dots D_{r_l,0} \in \mathcal{L}_{s_0-1}(v_0)A_{sep} + t^{(s+1)r^*} J_{s+1}(O_{sep}) + J_{s_0}.$$

As a corollary of the above Proposition we obtain the following equivalence:

$$\mathcal{F}E_0 \equiv (\mathcal{F}'^{(q)} + X(s_0-1))E_0 \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1} \right).$$

7.9.2. Calculation of $X(s_0-1)E_0$.

We write $X(s_0-1)$ in the following form: $X(s_0-1)\equiv$

$$\equiv \sum_{\substack{1\leqslant t\leqslant m<s_0\\ 0\leqslant n_1,\dots,n_m<N\\ r_1,\dots,r_m\in R}} \mathcal{F}^{t*(p^{n_t})}(-1)^{m+t+1}B_t^*(r_1,n_1,\dots,r_m,n_m)\left[t_1^{q\left(\frac{r_1}{p^{n_t 1}}+\dots+\frac{r_m}{p^{n_t m}}\right)}(e_1^{r_t}-1)\right]^{p^{n_t}}\times$$

$$\times\, e_1^{r_{t+1}p^{n_{t+1}}}\dots e_1^{r_m p^{n_m}}D_{r_1,n_1}\dots D_{r_m,n_m}(\mathrm{mod}\, J_{s_0}).$$

For fixed m we have:

$$E_0=\sum_{\substack{m<s<m+s_0\\ r_{m+1},\dots,r_s\in R}}\eta(r_{m+1},\dots,r_s)t_1^{q(r_{m+1}+\dots+r_s)}e_1^{r_{m+1}}\dots e_1^{r_s}D_{r_{m+1},0}\dots D_{r_s,0}(\mathrm{mod}\, J_{s_0}).$$

This can be written in the following form:

$$E_0=\sum_{\substack{m<s<m+s_0\\ r_{m+1},\dots,r_s\in R\\ 0\leqslant n_{m+1,s},\dots,n_{s-1,s}<N}}\eta(r_{m+1},n_{m+1,s},\dots,r_s,n_{ss})t_1^{q(r_{m+1}+\dots+r_s)}\times$$

$$\times e_1^{r_{m+1}p^{n_{m+1,s}}}\dots e_1^{r_s p^{n_{ss}}}D_{r_{m+1},n_{m+1,s}}\dots D_{r_s,n_{ss}}(\mathrm{mod}\, J_{s_0}),$$

because

$$\eta(r_{m+1},n_{m+1,s},\dots,r_s,n_{ss})=\begin{cases}\eta(r_{m+1},\dots,r_s), & \text{for } n_{m+1}=\dots=n_s,\\ 0, & \text{otherwise.}\end{cases}$$

Therefore,

$$X(s_0-1)E_0\equiv$$

$$\equiv\sum_{\substack{1\leqslant t\leqslant m<s<s_0\\ 0\leqslant n_{1s},\dots,n_{s-1,s}<N\\ n_{m+1,s}=\dots=n_{s-1,s}=0\\ r_1,\dots,r_s\in R}}\mathcal{F}^{t*(p^{n_{ts}})}(-1)^{m+t+1}B_t^*(r_1,n_{1s},\dots,r_s,n_{ms})\eta(r_{m+1},\dots,r_s)\times$$

$$\times\left[t_1^{q\left(\frac{r_1}{p^{n_t 1}}+\dots+\frac{r_s}{p^{n_t s}}\right)}(e_1^{r_t}-1)\right]^{p^{n_{ts}}}e_1^{r_{t+1}p^{n_{t+1,s}}}\dots e_1^{r_s p^{n_{ss}}}\times$$

$$\times D_{r_1,n_{1,s}}\dots D_{r_s,n_{s,s}}(\mathrm{mod}\, J_{s_0+1})$$

(multiplying $X(s_0-1)$ by the component of E_0 with index s we use indices $n_{1s},\dots,n_{ms}$ in the expression of $X(s_0-1)$).

7.9.3. Calculation of $\mathcal{F}'^{(q)}E_0$.

We use the convention that the empty sum is equal to 1. Then

$$\mathcal{F}'^{(q)} = \mathcal{F}'^{*} \sum_{\substack{1\leqslant m<s_0 \\ 0<n_1\dots n_{m-1}<N \\ r_1,\dots,r_{m-1}\in R}} t_1^{r_1p^{n_1}+\dots+r_{m-1}p^{n_{m-1}}}\eta(r_1,n_1,\dots,r_{m-1},n_{m-1})\times$$

$$\times D_{r_1,n_1}\dots D_{r_{m-1},n_{m-1}} (\operatorname{mod} J_{s_0}).$$

For fixed m we have:

$$E_0 = E_0'^{(q)} + \sum_{\substack{m\leqslant t\leqslant s<m+s_0 \\ r_m,\dots,r_s\in R}} t_1^{q(r_m+\dots+r_s)}\eta(r_m,\dots,r_s)(e_1^{r_t}-1)e_1^{r_{t+1}}\dots e_1^{r_s}D_{r_m,0}\dots D_{r_s,0}$$

and, as before, this may be written in a form:

$$E_0 = E_0'^{(q)} + \sum_{\substack{m\leqslant t\leqslant s<m+s_0 \\ r_1,\dots,r_s\in R}} t_1^{q(r_m+\dots+r_s)}\eta(r_m,n_{m,s},\dots,r_s,n_{ss})\times$$

$$\times(e_1^{r_t}-1)^{p^{n_{t,s}}} e_1^{r_{t+1}p^{n_{t+1,s}}}\dots e_1^{r_sp^{n_{ss}}} D_{r_m,n_{ms}}\dots D_{r_s,n_{ss}}.$$

Therefore,

$$\mathcal{F}'^{(q)}E_0 = (\mathcal{F}'E_0')^{(q)} +$$

$$+\sum_{\substack{1\leqslant m\leqslant t\leqslant s\leqslant s_0 \\ n_{1s},\dots,n_{m-1,s}\neq 0 \\ r_1,\dots,r_s\in R}} \mathcal{F}'^{*}\eta(r_1,n_{1s},\dots,r_{m-1},n_{m-1,s})\eta(r_{m+1},n_{m+1,s},\dots,r_s,n_{s,s})\left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}}+\dots+\frac{r_t}{p^{n_{ts}}}\right)}\right]^{p^{n_{ts}}}$$

$$\times(e_1^{r_t}-1)^{p^{n_{ts}}} e_1^{r_{t+1}p^{n_{t+1,s}}}\dots e_1^{r_sp^{n_{ss}}} D_{r_1,n_{1s}}\dots D_{r_s,n_{ss}} (\operatorname{mod} J_{s_0+1}).$$

We remark, that

$$\sum_{1\leqslant m\leqslant t} \eta(r_1,n_{1s},\dots,r_{m-1},n_{m-1,s})|_{n_{1s},\dots,n_{m-1,s}\neq 0}\,\eta(r_m,n_{m+1,s},\dots,r_s,n_{ss}) =$$

$$= \tilde{\eta}(r_s,n_s,\dots,r_1,n_1)|_{n_t=\dots=n_s}.$$

7.9.4. We can apply the identity of proposition n.7.5.7 to calculate the sum of $\mathcal{F}'^{(q)}E_0$ and XE_0. We obtain:

$$\mathcal{F}E_0 \equiv \sum_{\substack{1\leqslant t\leqslant s\leqslant s_0 \\ 0\leqslant n_1,\dots,n_s<N \\ r_1,\dots,r_s\in R}} \mathcal{F}'^{*(p^{n_{ts}})}(-1)^{s+t}B_t(r_1,n_1,\dots,r_s,n_s)\times$$

$$\times\left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}}+\dots+\frac{r_t}{p^{n_{ts}}}\right)}(e_1^{r_t}-1)\right]^{p^{n_{ts}}} e_1^{r_{t+1}p^{n_{t+1,s}}}\dots e_1^{r_sp^{n_{ss}}}\times$$

$$\times D_{r_1,n_{1,s}}\dots D_{r_s,n_{s,s}} (\operatorname{mod} J_{s_0+1}).$$

Therefore,

$$\mathcal{F}^{(q)} - \mathcal{F} = \left[\mathcal{F}'^{(q)} - \mathcal{F}'\right]^{(q)} + A_1 \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1} \right),$$

where

$$A_1 \equiv \sum_{\substack{1\leqslant t\leqslant s\leqslant s_0\\ 0\leqslant n_1,\dots,n_s<N\\ r_1,\dots,r_s\in R}} \mathcal{F}'^{*(p^{n_{ts}+n_s})}(-1)^{s+t} B_t(r_1,n_1,\dots,r_s,n_s)\times$$

$$\times \left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}}+\dots+\frac{r_t}{p^{n_{ts}}}\right)}(e_1^{r_t}-1)\right]^{p^{n_{ts}+n_s}} e_1^{r_{t+1}p^{n_{t+1,s}+n_s}} \dots e_1^{r_s p^{n_{ss}+n_s}} \times$$

$$\times D_{r_1,n_1}\dots D_{r_s,n_s} (\bmod J_{s_0+1}).$$

7.10. Let $X_1 \in A_{K_{sep}}$ be such, that $X_1^{(q)} - X_1 = A_1$. Then the above calculation gives

$$\mathcal{F} = \mathcal{F}'^{(q)} + X_1 \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1} \right).$$

Let I be any ideal of the Lie algebra $\mathcal{L}$ such that $I \supset C_{s_0+1}(\mathcal{L})$. It is clear from Proposition of n.7.2, that $\mathcal{L}_{s_0}(v_0)$ is the minimal element in the subset of such ideals having the following property:

the field of definition of $\mathcal{F} \bmod (IA_{sep} + J_{s_0+1})$ *has the upper ramification numbers* $< v_0$.

By induction we can assume that $I \supset (\mathcal{L}_{s_0-1}(v_0)J_1) \cap \mathcal{L}$.

Proposition. *$\mathcal{L}_{s_0}(v_0)$ is the minimal element in the set of all ideals of the Lie algebra $\mathcal{L}$ such that*

(a) $IA_{sep} \supset \mathcal{L}_{s_0-1}(v_0)J_1 + J_{s_0+1}$;

(b) field of definition of $X_1 \bmod (IA_{sep} + J_{s_0+1})$ has the upper ramification numbers $< v_0$.

Proof.

It is clear that $\mathcal{L}_{s_0}(v_0)$ satisfies the condition (a) of the proposition.

Let I be an arbitrary ideal of $\mathcal{L}$ satisfying (a). Let $\mathcal{F} = \mathcal{F}'^{(q)} + Y_1$. Then

$$X_1 \equiv Y_1 \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1} \right).$$

The field of definition of $X_1 \bmod (IA_{sep} + J_{s_0+1})$ has largest ramification numbers $< v_0$ if and only if the field of definition of $Y_1 \bmod (IA_{sep} + J_{s_0+1})$ has the largest ramification numbers $< v_0$. Let $\mathcal{L}(I)$ be the field of definition of $Y_1 \bmod (IA_{sep} +$

$J_{s_0+1})$ and $K(I)$ be the field of definition of $\mathcal{F} \bmod (IA_{sep} + J_{s_0+1}))$, then $K'(I) := f(K(I))$ will be the field of definition of $\mathcal{F}' \bmod (IA_{sep} + J_{s_0+1})$ (isomorphism $f : K_{sep} \longrightarrow K'_{sep}$ was defined in n.7.6). The equality $\mathcal{F} = \mathcal{F}'^{(q)} + Y_1$ gives $K(I) \subset K'(I)L(I)$ and $L(I) \subset K(I)K'(I)$. So, our proposition follows from Lemma 7.4.2.

7.11. Some calculations.

7.11.1. Let (c.f. n.7.7(c))

$$X(s_0) = \sum_{\substack{1 \leqslant t \leqslant s \leqslant s_0 \\ 0 \leqslant n_1, \dots, n_s < N \\ r_1, \dots, r_s \in R}} \mathcal{F}'^{*(p^{n_t})} (-1)^{s+t} B_t^*(r_1, n_1, \dots, r_s, n_s) \times$$

$$\times \left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}} + \dots + \frac{r_t}{p^{n_{ts}}}\right)} (e_1^{r_t} - 1) \right]^{p^{n_t}} e_1^{r_{t+1} p^{n_{t+1}}} \dots e_1^{r_s p^{n_s}} D_{r_1, n_1} \dots D_{r_s, n_s}.$$

This sum consists of all members of the above expression for A_1 which satisfy the additional condition $n_t \geqslant n_s$.

Let $X_1 = X(s_0) + X_1'$, then

$$X_1'^{(q)} - X_1' = A_1 - \left(X(s_0)^{(q)} - X(s_0) \right) = A_1',$$

where $A_1' \equiv$

$$\equiv \sum_{\substack{1 \leqslant t \leqslant s \leqslant s_0 \\ 0 \leqslant n_1, \dots, n_s < N \\ r_1, \dots, r_s \in R}} \mathcal{F}'^{*(p^{n_t+N})} (-1)^{s+t+1} B_t(r_1, n_1, \dots, r_s, n_s) \left[t_1^{q\left(\frac{r_1}{p^{n_{t1}}} + \dots + \frac{r_t}{p^{n_{ts}}}\right)} (e_1^{r_t} - 1) \right]^{p^{n_t+N}} \times$$

$$\times e_1^{r_{t+1} p^{n_t + N - n_{t,t+1}}} \dots e_1^{r_s p^{n_t + N - n_{t,s}}} D_{r_1, n_1} \dots D_{r_s, n_s} (\bmod J_{s_0+1}).$$

It is easy to see that

$$A_1' \equiv \sum_{0 \leqslant m < N} \left[\mathcal{F}'^{*(q)} A(s_0)_0 \right]^{(p^m)},$$

where $A(s_0)_0$ is given by the formula in n.7.7(d) with $s^* = s_0$.

Lemma.

$$\mathcal{F}'^* - 1 \in \mathcal{L}_{s_0-1}(v_0) A_{sep} + \sum_{1 \leqslant s < s_0} t_1^{r^* s} J_s(O_{sep}) + J_{s_0}.$$

Proof. This follows from the equality $\mathcal{F}'^* = \mathcal{F}'^{(p)}$, the equivalence $\mathcal{F}'^{(p)} \equiv \mathcal{F}' E' \bmod J_p$ (c.f. n.7.6) and Proposition 7.9.1.

From this lemma and inductive assumption 7.7(d) it follows, that

$$\sum_{0 \leqslant m < N} \left[\mathcal{F}'^{*(q)} - 1 \right]^{p^m} A(s_0)_0^{(p^m)} \in \mathcal{L}_{s_0-1}(v_0) J_1 + \sum_{1 \leqslant s \leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1}$$

(we use, that $A(s_0)_0 \equiv A(s_0-1)_0 \bmod J_{s_0}$), therefore,

$$A_1' \equiv \sum_{0\leqslant m<N} A(s_0)_0^{(p^m)} \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)}J_s(O_{sep}) + J_{s_0+1}\right).$$

Let $X_1'' \in A_{sep}$ be such that

$$X_1''^{(q)} - X_1'' = \sum_{0\leqslant m<N} A(s_0)_0^{(p^m)}.$$

Obviously,

$$X_1'' \equiv X_1' \bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)}J_s(O_{sep}) + J_{s_0+1}\right).$$

and we have the following reduction:

Proposition. *$\mathcal{L}_{s_0}(v_0)$ is the minimal element in the set of all ideals of the Lie algebra $\mathcal{L}$ such that*

(a) $IA_{sep} \supset \mathcal{L}_{s_0-1}(v_0)J_1 + J_{s_0+1}$;

(b) field of definition of $X_1'' \bmod(IA_{sep}+J_{s_0+1})$ has the upper ramification numbers $< v_0$.

7.11.2. We remark, that $B_t(r_1,n_1,...,r_s,n_s)$ and $D_{r_1,n_1},...,D_{r_s,n_s}$ depend on the residues of $n_1,...,n_s$ modulo N. We change indices in the above expression of $A(s_0)_0$. In every summand we introduce new indices: we use the index n_l instead of $N-n_{tl}=n_{lt}^*$. Then $B_t(r_1,n_1,...,r_s,n_s) = B_t(r_1,n_{1t}^*,...,r_s,n_{st}^*)$ goes to $B_t(r_1,n_1,...,r_s,n_s)$ and one can rewrite the expression for $A(s_0)_0$ in the following form:

$$A(s_0)_0 = \sum_{\gamma\in\mathbf{Q}} A(\gamma)_0\,[t_1^{q\gamma}]^q,$$

where

$$A(\gamma)_0 = \sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant N\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{N-n_1}}+...+\frac{r_s}{p^{N-n_s}}=\gamma}} \sum_{\substack{1\leqslant t\leqslant s\\ n_t=N}} (-1)^{s+t}B_t(r_1,n_1,...,r_s,n_s)\times$$

$$\times(e_1^{r_t}-1)^{p^{n_t}}e_1^{r_{t+1}p^{n_{t+1}}}...e_1^{r_sp^{n_s}}D_{r_1,n_1}...D_{r_s,n_s}.$$

7.11.3. For a positive rational number γ and a natural number n^* such that $0<n^*\leqslant N$, we introduce the elements A_{γ,n^*} of $A_{K_{tr}}$ given by the following expression:

$$A_{\gamma,n^*} = \sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant n^*\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{n_{*1}}}+...+\frac{r_s}{p^{n_{*s}}}=\gamma}} \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=...=n_{t_2}=n^*\\ n_{t_1-1},n_{t_2+1}\neq n^*}} (-1)^{s+t}B_t(r_1,n_1,...,r_s,n_s)\times$$

$$\times\left[(e_1^{r_t}-1)e_1^{r_{t+1}+...+r_{t_2}}\right]^{p^{n^*}} D_{r_1,n_1}...D_{r_s,n_s}$$

(we use an abreviation $n_{*l}=n_*-n_l\in[0,N)$ for $1\leqslant l\leqslant s$).

Proposition.

$$A(\gamma)_0 \equiv \left(A_{\gamma,N} + \sum_{\substack{N>m_1>0\\ \gamma_0,\gamma_1\in\mathbb{Q}\\ \gamma_0+\frac{\gamma_1}{p^{N-m_1}}=\gamma}} A_{\gamma_0,N}A_{\gamma_1,m_1} + \sum_{\substack{N>m_1>m_2>0\\ \gamma_0,\gamma_1,\gamma_2\in\mathbb{Q}\\ \gamma_0+\frac{\gamma_1}{p^{N-m_1}}+\frac{\gamma_2}{p^{N-m_2}}=\gamma}} A_{\gamma_0,N}A_{\gamma_1,m_1}A_{\gamma_2,m_2} + \dots \right) \bmod J_{s_0+1}.$$

Proof. For any collection $(r_1, n_1, ..., r_s, n_s)$, where $r_1, ..., r_s \in R, 0 < n_1, ..., n_s \leqslant N$, and index t, such that $t \leqslant t_2$, where $n_{t_2} = n^* := \max\{n_1, ..., n_s\}, n_{t_2+1} \neq n^*$, we set

$$A^{(1)}(r_1, n_1, ..., r_s, n_s; t) =$$

$$= (-1)^{s+t} B_t(r_1, n_1, ..., r_{t_2}, n_{t_2})\eta^*(r_{t_2+1}, n_{t_2+1}, ..., r_s, n_s) \left[(e_1^{r_t} - 1)e_1^{r_{t+1}+\dots+r_{t_2}}\right]^{p^{n^*}}$$

Remark.

If the index t_2 is not uniquely defined, then all the $A^{(1)}(r_1, n_1, ..., r_s, n_s; t)$ are automatically equal to 0.

From the definition of the constants $B_t(r_1, n_1, ..., r_s, n_s)$ (c.f. n.7.5.4) it follows that

$$B_t(r_1, n_1, ..., r_s, n_s) = B_t(r_1, n_1, ..., r_{t_2}, n_{t_2})\eta^*(r_{t_2+1}, n_{t_2+1}, ..., r_s, n_s)$$

and, therefore,

$$A_{\gamma_0,N} = \sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant N\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{N-n_1}}+\dots+\frac{r_s}{p^{N-n_s}}=\gamma_0}} \sum_{\substack{1\leqslant t\leqslant t_2\\ n_{t_2}=N\\ n_{t_2+1}\neq N}} A^{(1)}(r_1, n_1, ..., r_s, n_s; t) D_{r_1,n_1} \dots D_{r_s,n_s}.$$

Let $r_1, ..., r_s \in R, n_1, ..., n_s \in \mathbb{N}$. If $n^* = \max\{n_1, ..., n_s\}$, $n_i = n^*$ for $t_1 \leqslant i \leqslant t_2$ and $n_{t_1-1}, n_{t_2+1} \neq n^*$, then we obtain the following identity from lemma n.7.5.5 :

$$\sum_{t_1\leqslant t\leqslant t_2} (-1)^t B_t(r_1, n_1, ..., r_s, n_s) \left[e_1^{r_t+\dots+r_{t_2}} - e_1^{r_{t+1}+\dots+r_{t_2}}\right] =$$

$$= \sum_{1\leqslant t\leqslant t_2} (-1)^t \eta^*(r_{t-1}, n_{t-1}, ..., r_1, n_1)\eta^*(r_t, n_t, ..., r_s, n_s) \left(e_1^{r_t+\dots+r_{t_2+1}} - 1\right).$$

For fixed index s, and any collection $(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}})$ and an index u such that $s + 1 \leqslant u \leqslant u_2$, where $n_{u_2} = n^* := \max\{n_{s+1}, ..., n_{\hat{s}}\}, n_{u_2+1} \neq n^*$, we set

$$A^{(2)}(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}}; u) =$$

$$= (-1)^{\hat{s}+u} \eta^*(r_{u-1}, n_{u-1}, ..., r_{s+1}, n_{s+1})\eta^*(r_u, n_u, ..., r_{\hat{s}}, n_{\hat{s}}) \left[e_1^{r_u+\dots+r_{u_2}} - 1\right]^{p^{n^*}}.$$

Now the above identity means that

$$A_{\gamma_1,n^*}=\sum_{\substack{s+1\leqslant \hat{s}\leqslant s+s_0\\ 0<n_{s+1},\dots,n_{\hat{s}}\leqslant n^*\\ r_{s+1},\dots,r_{\hat{s}}\in R\\ \frac{r_{s+1}}{p^{n^*-n_{s+1}}}+\dots+\frac{r_{\hat{s}}}{p^{n^*-n_{\hat{s}}}}=\gamma_1}}\ \sum_{\substack{s+1\leqslant u\leqslant u_2\\ n_{u_2}=n^*\\ n_{u_2+1}\neq n^*}}(-1)^{\hat{s}+u}A^{(2)}(r_{s+1},n_{s+1},\dots,r_{\hat{s}},n_{\hat{s}};u)D_{r_{s+1},n_{s+1}}\dots D_{r_{\hat{s}},n_{\hat{s}}}.$$

The coefficient of $D_{r_1,n_1}\dots D_{r_{\hat{s}},n_{\hat{s}}}$ in the expression of $\sum\limits_{\gamma_0,\gamma_1}A_{\gamma_0,N}A_{\gamma_1,n^*}$ is equal to the sum $\sum\limits_{t<u}C_{t,u}$, where

$$C_{t,u}=A^{(1)}(r_1,n_1,\dots,r_t,n_t;t)A^{(2)}(r_{t+1},n_{t+1},\dots,r_{\hat{s}},n_{\hat{s}};u)+$$

$$+A^{(1)}(r_1,n_1,\dots,r_{t+1},n_{t+1};t)A^{(2)}(r_{t+2},n_{t+2},\dots,r_{\hat{s}},n_{\hat{s}};u)+\dots$$

$$\dots+A^{(1)}(r_1,n_1,\dots,r_{u-1},n_{u-1};t)A^{(2)}(r_u,n_u,\dots,r_{\hat{s}},n_{\hat{s}};u).$$

For $u\neq t_2$ we have the following identity:

$$\sum_{t_2\leqslant s<u}\eta^*(r_{t_2+1},n_{t_2+1},\dots,r_s,n_s)\eta^*(r_{u-1},n_{u-1},\dots,r_{s+1},n_{s+1})=0,$$

c.f. n.7.5.5. This means that $C_{t,u}=0$, if $t+1\neq u$.
Therefore,

$$\sum_{\substack{\gamma_0,\gamma_1\\ \gamma_0+\frac{\gamma_1}{p^{N-n^*}}=\gamma}}A_{\gamma_0,N}A_{\gamma_1,n^*}\equiv$$

$$\equiv\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,\dots,n_s\leqslant N\\ r_1,\dots,r_s\in R\\ \frac{r_1}{p^{N-n_1}}+\dots+\frac{r_s}{p^{N-n_s}}=\gamma_0}}(-1)^s\sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=\dots=n_{t_2}=N\\ n_{t_2+1}=\dots=n_{t_3}=n^*\\ n_{t_1-1}<N\\ n_{t_3+1}<n^*}}(-1)^tB_t(r_1,n_1,\dots,r_{t_2},n_{t_2})\left[(e_1^{r_t}-1)e_1^{r_{t+1}+\dots+r_{t_2}}\right]^{p^N}\times$$

$$\times\eta^*(r_{t_2+1},n_{t_2+1},\dots,r_{t_3},n_{t_3})\left[e_1^{r_{t_2+1}+\dots+r_{t_3}}-1\right]^{p^{n^*}}D_{r_1,n_1}\dots D_{r_s,n_s}\bmod J_{s_0+1}.$$

Now we obtain, that

$$A_{\gamma,N}+\sum_{\substack{N>m_1>0\\ \gamma_0,\gamma_1\\ \gamma_0+\frac{\gamma_1}{p^{N-m_1}}=\gamma}}A_{\gamma_0,N}A_{\gamma_1,m_1}\equiv$$

$$\equiv\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,\dots,n_s\leqslant N\\ r_1,\dots,r_s\in R\\ \frac{r_1}{p^{N-n_1}}+\dots+\frac{r_s}{p^{N-n_s}}=\gamma_0}}\ \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=\dots=n_{t_2}=N\\ n_{t_2+1}=\dots=n_{t_3}=m_1\\ n_{t_1-1}\neq N\\ n_{t_3+1}\neq m_1}}(-1)^{s+t}B_t(r_1,n_1,\dots,r_s,n_s)\times$$

$$\times \left[(e_1^{r_t}-1)e_1^{r_{t+1}+\ldots+r_{t_2}}\right]^{p^N} \left[e_1^{r_{t_2+1}}\ldots e_1^{r_{t_s}}\right]^{p^{m_1}} D_{r_1,n_1}\ldots D_{r_s,n_s} \bmod J_{s_0+1}.$$

Proceeding in the same manner, we obtain our proposition.

7.11.4. Let

$$B_{\gamma,n^*} = \sum_{\substack{1\leqslant s\leqslant s_0\\ n_1=\ldots n_s=n^*\\ r_1,\ldots,r_s\in R\\ r_1+\ldots+r_s=\gamma}} \sum_{1\leqslant t\leqslant s}(-1)^{s+t}B_t(r_1,n_1,\ldots,r_s,n_s)\left[(e_1^{r_t}-1)e_1^{r_{t+1}+\ldots+r_s}\right]^{p^{n^*}} D_{r_1,n_1}\ldots D_{r_s,n_s}.$$

$$C^{(1)}_{\gamma,n^*} = \sum_{\substack{1\leqslant s<s_0\\ 0<n_1,\ldots,n_s<n^*\\ r_1,\ldots,r_s\in R\\ \frac{r_1}{p^{n^*}1}+\ldots+\frac{r_s}{p^{n^*s}}=\gamma}} \eta^*(r_s,n_s,\ldots,r_1,n_1)D_{r_1,n_1}\ldots D_{r_s,n_s}.$$

$$C^{(2)}_{\gamma,n^*} = \sum_{\substack{1\leqslant s<s_0\\ 0<n_1,\ldots,n_s<n^*\\ r_1,\ldots,r_s\in R\\ \frac{r_1}{p^{n^*}1}+\ldots+\frac{r_s}{p^{n^*s}}=\gamma}} (-1)^s\eta^*(r_1,n_1,\ldots,r_s,n_s)D_{r_1,n_1}\ldots D_{r_s,n_s}$$

By the definition we set $C^{(1)}_{0,n^*}=C^{(2)}_{0,n^*}=0$.

Proposition.

$$A_{\gamma,n^*} = \sum_{\substack{\gamma_1,\gamma_0,\gamma_2\in\mathbb{Q}\\ \gamma_1+\gamma_0+\gamma_2=\gamma}} C^{(1)}_{\gamma_1,n^*}B_{\gamma_0,n^*}C^{(2)}_{\gamma_2,n^*}.$$

Proof.

It is sufficient to remark, that

if $r_1,\ldots,r_s\in R, n_1,\ldots,n_s\in\mathbb{N}, n_i=n^*=\max\{n_1,\ldots,n_s\}$ for $t_1\leqslant i\leqslant t_2$ and $n_{t_1-1},n_{t_2+1}\neq n^*$, then for $t_1\leqslant t\leqslant t_2$ we have:

$$B_t(r_1,n_1,\ldots,r_s,n_s)=$$

$$=\eta^*(r_{t_1-1},n_{t_1-1},\ldots,r_1,n_1)B_{t-t_1+1}(r_{t_1},n_{t_1},\ldots,r_{t_2},n_{t_2})\eta^*(r_{t_2+1},n_{t_2+1},\ldots,r_s,n_s).$$

7.11.5. Consider the expression for A_{γ,n^*} from n.7.11.3. Since

$$e_1=\widetilde{exp}\left(-\frac{1}{r^*}t_1^{-r^*(q-1)}\right)\in\mathbb{F}_p\left[t_1^{-r^*(q-1)}\right]$$

we can present A_{γ,n^*} as a power series of variable $t_1^{-r^*(q-1)}$:

$$A_{\gamma,n^*}=\sum_{m\geqslant1}A_{\gamma,n^*}(m)\left[t_1^{-r^*(q-1)}\right]^{mp^{n^*}}.$$

The coefficients $A_{\gamma,n^*}(m)$, where $1 \leqslant m < p$, depend only on the residue $A_{\gamma,n^*} \bmod \left[t_1^{-pr^*(q-1)}\right]^{p^{n^*}} J_1(O_{sep})$. Therefore, they can be computed by means of the following equivalences:

$$e_1^{r_t+\ldots+r_{t_2}} \equiv \widetilde{exp}\left(-\frac{r_t+\ldots+r_{t_2}}{r^*}t_1^{-r^*(q-1)}\right) \bmod \left[t_1^{-pr^*(q-1)}\right]^{p^{n^*}} O'_{tr}.$$

The same remark can be done for the coefficients $B_{\gamma,n^*}(m)$, $1 \leq m < p$, of the expression

$$B_{\gamma,n^*} = \sum_{m\geqslant 1} B_{\gamma,n^*}(m)\left[t_1^{-r^*(q-1)}\right]^{mp^{n^*}}.$$

Proposition. *Let* $1 \leq m \leq p-2$. *Then*

$$\sum_{\substack{\gamma_1,\gamma_2\in\mathbf{Q}\\ \gamma_1+\gamma_2=\gamma}} A_{\gamma_1,n^*}(1)A_{\gamma_2,n^*}(m) \equiv (m+1)A_{\gamma,n^*}(m+1)-$$

$$-\sum_{\substack{\gamma_1,\gamma_0,\gamma_2\in\mathbf{Q}\\ \gamma_1+\gamma_0+\gamma_2=\gamma}} C^{(1)}_{\gamma_1,n^*}\gamma_0 B_{\gamma_0,n^*}(m)C^{(2)}_{\gamma_2,n^*} \bmod J_{s_0+1}.$$

Proof.
We have: $A_{\gamma,n^*}(1) =$

$$=\frac{(-1)}{1!r^*}\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,\ldots,n_s\leqslant n^*\\ r_1,\ldots,r_s\in R\\ \frac{r_1}{p^{n_1}}+\ldots+\frac{r_s}{p^{n_s}}=\gamma}}\ \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=\ldots=n_{t_2}=n^*\\ n_{t_1-1},n_{t_2+1}\neq n^*}}(-1)^{s+t}B_t(r_1,n_1,\ldots,r_s,n_s)r_tD_{r_1,n_1}\ldots D_{r_s,n_s}.$$

From the lemma of n.7.5.5 we obtain the following identity:

$$\sum_{t_1\leqslant t\leqslant t_2}(-1)^tB_t(r_1,n_1,\ldots,r_s,n_s)r_t =$$

$$=\sum_{t_1\leqslant t\leqslant t_2}(-1)^t\eta^*(r_t,n_t,\ldots,r_1,n_1)\eta^*(r_{t+1},n_{t+1},\ldots,r_s,n_s)(r_{t_1}+\ldots+r_t).$$

For any collection $(r_1,n_1,\ldots,r_s,n_s)$ and index t such that $t \geqslant t_1$, where $n_{t_1} = n^* := \max\{n_1,\ldots,n_s\}, n_{t_1+1} \neq n^*$, we set

$$E^{(1)}(r_1,n_1,\ldots,r_s,n_s;t) =$$

$$=(-1)^{s+t}\eta^*(r_t,n_t,\ldots,r_1,n_1)\eta^*(r_{t+1},n_{t+1},\ldots,r_s,n_s)(r_{t_1}+\ldots+r_t).$$

Remark.

If the index t_1 is not uniquely defined, then the above expression for $E^{(1)}(r_1, n_1, ..., r_s, n_s; t)$ is automatically equal to 0.
Then we have: $A_{\gamma,n^*}(1) =$

$$= \frac{(-1)}{1!r^*} \sum_{\substack{1 \leqslant s \leqslant s_0 \\ 0 < n_1, ..., n_s \leqslant n^* \\ r_1, ..., r_s \in R \\ \frac{r_1}{p^{n_{*1}}} + ... + \frac{r_s}{p^{n_{*s}}} = \gamma_1}} \sum_{\substack{t_1 \leqslant t \leqslant s \\ n_{t_1} = n^* \\ n_{t_1 - 1} \neq n^*}} (-1)^{s+t} E^{(1)}(r_1, n_1, ..., r_s, n_s; t) D_{r_1,n_1} ... D_{r_s,n_s}.$$

For fixed index s consider the expression for $A_{\gamma_2,n^*}(m)$ in the following form:

$$A_{\gamma_2,n^*}(m) = \frac{(-1)^m}{m!r^{*m}} \sum_{\substack{s+1 \leqslant \hat{s} \leqslant s+s_0 \\ 0 < n_{s+1}, ..., n_{\hat{s}} \leqslant n^* \\ r_{s+1}, ..., r_{\hat{s}} \in R \\ \frac{r_{s+1}}{p^{n_{*s+1}}} + ... + \frac{r_{\hat{s}}}{p^{n_{*\hat{s}}}} = \gamma_2}} \sum_{\substack{u_1 \leqslant u \leqslant u_2 \\ n_{u_1} = ... = n_{u_2} = n^* \\ n_{u_1 - 1}, n_{u_2 + 1} \neq n^*}} (-1)^{\hat{s}+u} B_{u-s}(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}}) \times$$

$$\times \left[(r_u + ... + r_{u_2})^m - (r_{u+1} + ... + r_{u_2})^m\right] D_{r_{s+1},n_{s+1}} ... D_{r_{\hat{s}},n_{\hat{s}}}.$$

As earlier, we have an identity:

$$\sum_{u_1 \leqslant u \leqslant u_2} (-1)^u B_{u-s}(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}}) \left[(r_u + ... + r_{u_2})^m - (r_{u+1} + ... + r_{u_2})^m\right] =$$

$$= \sum_{s+1 \leqslant u \leqslant u_2} (-1)^u \eta^*(r_{u-1}, n_{u-1}, ..., r_{s+1}, n_{s+1}) \eta^*(r_u, n_u, ..., r_{\hat{s}}, n_{\hat{s}})(r_u + ... + r_{u_2})^m.$$

For some fixed index s, any collection $(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}})$ and an index u such that $s + 1 \leqslant u \leqslant u_2$, where $n_{u_2} = n^* = \max\{n_{s+1}, ..., n_{\hat{s}}\}, n_{u_2+1} \neq n^*$, we set:

$$E^{(2)}(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}}) =$$

$$= (-1)^{u+\hat{s}} \eta^*(r_{u-1}, n_{u-1}, ..., r_{s+1}, n_{s+1}) \eta^*(r_u, n_u, ..., r_{\hat{s}}, n_{\hat{s}})(r_u + ... + r_{u_2})^m.$$

Then, $A_{\gamma_2,n^*}(m) =$

$$= \frac{(-1)^m}{m!r^{*m}} \sum_{\substack{s+1 \leqslant \hat{s} \leqslant s+s_0 \\ 0 < n_{s+1}, ..., n_{\hat{s}} \leqslant n^* \\ r_{s+1}, ..., r_{\hat{s}} \in R \\ \frac{r_{s+1}}{p^{n_{*s+1}}} + ... + \frac{r_{\hat{s}}}{p^{n_{*\hat{s}}}} = \gamma_2}} \sum_{\substack{s+1 \leqslant u \leqslant u_2 \\ n_{u_2} = n^* \\ n_{u_2+1} \neq n^*}} E^{(2)}(r_{s+1}, n_{s+1}, ..., r_{\hat{s}}, n_{\hat{s}}) D_{r_{s+1},n_{s+1}} ... D_{r_{\hat{s}},n_{\hat{s}}}.$$

Now the coefficient for $D_{r_1,n_1} ... D_{r_{\hat{s}},n_{\hat{s}}}$ in the expression of the sum $\sum_{\gamma_1,\gamma_2} A_{\gamma_1,n^*}(1) A_{\gamma_2,n^*}(m)$ is equal to $\sum_{t<u} F_{t,u}$, where

$$F_{t,u} = E^{(1)}(r_1, n_1, ..., r_t, n_t; t) E^{(2)}(r_{t+1}, n_{t+1}, ..., r_{\hat{s}}, n_{\hat{s}}; u) +$$

$$+E^{(1)}(r_1,n_1,...,r_{t+1},n_{t+1};t)E^{(2)}(r_{t+2},n_{t+2},...,r_{\bar{s}},n_{\bar{s}};u)+...$$
$$...+E^{(1)}(r_1,n_1,...,r_{u-1},n_{u-1};t)E^{(2)}(r_u,n_u,...,r_{\bar{s}},n_{\bar{s}};u).$$

As earlier, we obtain, that $F_{t,u}=0$, if $u\neq t+1$. Therefore,

$$\sum_{\substack{\gamma_1,\gamma_2\\ \gamma_1+\gamma_2=\gamma}} A_{\gamma_1,n^*}(1)A_{\gamma_2,n^*}(m)=$$

$$=\frac{(-1)^{m+1}}{m!r^{*m}}\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant n^*\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{n_1}}+...+\frac{r_s}{p^{n_s}}=\gamma}}\ \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=...=n_{t_2}=n^*\\ n_{t_1-1},n_{t_2+1}\neq n^*}}(-1)^{s+t}\eta^*(r_t,n_t,...,r_1,n_1)\times$$
$$\times\eta^*(r_{t+1},n_{t+1},...,r_s,n_s)(r_{t_1}+...+r_t)(r_{t+1}+...+r_{t_2})^m.$$

Now our proposition can be deduced from the following formulae:

$$A_{\gamma,n^*}(m+1)=\frac{(-1)^{m+1}}{(m+1)!r^{*m+1}}\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant n^*\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{n_1}}+...+\frac{r_s}{p^{n_s}}=\gamma}}\ \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=...=n_{t_2}=n^*\\ n_{t_1-1},n_{t_2+1}\neq n^*}}(-1)^{s+t}\eta^*(r_t,n_t,...,r_1,n_1)\times$$
$$\times\eta^*(r_{t+1},n_{t+1},...,r_s,n_s)(r_{t+1}+...+r_{t_2})^{m+1},$$

$$\sum_{\substack{\gamma_1,\gamma_0,\gamma_2\in\mathbf{Q}\\ \gamma_1+\gamma_0+\gamma_2=\gamma}} C^{(1)}_{\gamma_1,n^*}\gamma_0 B_{\gamma_0,n^*}(m)C^{(2)}_{\gamma_2,n^*}=$$

$$=\frac{(-1)^{m}}{m!r^{*m}}\sum_{\substack{1\leqslant s\leqslant s_0\\ 0<n_1,...,n_s\leqslant n^*\\ r_1,...,r_s\in R\\ \frac{r_1}{p^{n_1}}+...+\frac{r_s}{p^{n_s}}=\gamma}}\ \sum_{\substack{t_1\leqslant t\leqslant t_2\\ n_{t_1}=...=n_{t_2}=n^*\\ n_{t_1-1},n_{t_2+1}\neq n^*}}(-1)^{s+t}\eta^*(r_t,n_t,...,r_1,n_1)\times$$
$$\times\eta^*(r_{t+1},n_{t+1},...,r_s,n_s)(r_{t_1}+...+r_{t_2})(r_{t+1}+...+r_{t_2})^m.$$

7.12. Let $N_0=N(R,v_0)$ be the natural number from the Proposition 4.4.

Proposition. *If $n^*<N_0$, then*

$$A_{\gamma,n^*}\,[t_1^{q\gamma}]^{p^{n^*}}\in\mathcal{L}_{s_0-1}(v_0)A_{sep}+\sum_{1\leqslant s<s_0}\left[t^{sr^*}\right]^{p^{N_0}}J_s(O_{sep})+J_{s_0}.$$

Proof.

The arguments of the Lemma n.7.9.1 give the following lemma

Lemma. *If* $r_1 + \dots + r_s \geq s_1 r^*$, *then*

$$D_{r_1,n_1} \dots D_{r_s,n_s} \in \mathcal{L}_{s_0-1}(v_0) \otimes k + C_s \otimes k,$$

where $s = \min\{s_1 + 1, s_0\}$.

Then the slight modification of the proof of Proposition 7.9.1 implies our Proposition.

7.13. Proposition. *If* $\gamma \geq s_0 r^*$, *then*

$$A_{\gamma,n^*} [t_1^{q\gamma}]^{p^{n^*}} \equiv A_{\gamma,n^*}(1) \left[t_1^{q\gamma - r^*(q-1)}\right]^{p^{n^*}} \bmod (\mathcal{L}_{s_0-1}(v_0) J_1 + J_{s_0+1}).$$

Proof.

We have the following analogue of the Lemma n.7.12:

Lemma. *If* $s \geq 2$ *and* $r_1 + \dots + r_s \geq s_0 r^*$, *then*

$$D_{r_1,n_1} \dots D_{r_s,n_s} \in \mathcal{L}_{s_0-1}(v_0) J_1(O_{sep}) + J_{s_0+1}(O_{sep}).$$

Proof.

Let $(s+1)r^* > r_1 + \dots + r_s \geq s_1 r^*$. If $s_1 + 1 \geq s_0$, then

$$D_{r_1,n_1} \dots D_{r_{s-1},n_{s-1}} \in \mathcal{L}_{s_0-1}(v_0) \otimes k + J_{s_0},$$

therefore,

$$D_{r_1,n_1} \dots D_{r_s,n_s} \in \mathcal{L}_{s_0-1}(v_0) J_1(O_{sep}) + J_{s_0+1}(O_{sep}).$$

If $s_1 + 1 < s_0$, then we have $r_s \geq (s_0 - (s_1 + 1)) r^*$, therefore,

$$D_{r_s,n_s} \in \mathcal{L}_{s_0-1}(v_0) \otimes k + J_{s_0-s_1}(O_{sep})$$

and we obtain the conclusion of our Lemma.

From this Lemma it follows that

$$A_{\gamma,n^*} \equiv -\frac{\gamma}{r^*} D_{\gamma,n^*} \bmod (\mathcal{L}_{s_0-1}(v_0) J_1(O_{sep}) + J_{s_0+1}(O_{sep}))$$

($D_{\gamma,n^*} = 0$, if $\gamma \notin R$).

The same arguments show that

$$A_{\gamma,n^*}(1) \equiv -\frac{\gamma}{r^*} D_{\gamma,n^*} \bmod (\mathcal{L}_{s_0-1}(v_0) J_1(O_{sep}) + J_{s_0+1}(O_{sep})).$$

7.14. Proposition. *Let* $\gamma \leq s_0 r^*$, $n^* \geq N_0$. *Then*

$$A_{\gamma,n^*} [t_1^{q\gamma}]^q \equiv A_{\gamma,n^*}(1) \sum_{1 \leq m < p} \frac{(-\gamma)^{m-1}}{m!} \left[t_1^{q\gamma - r^*(q-1)}\right]^{p^{n^*}}$$

$$\bmod \left(\mathcal{L}_{s_0-1}(v_0) J_1 + \sum_{1 \leqslant s \leqslant s_0} \left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0+1} \right).$$

Proof.

7.14.1. Lemma. *Let $n^* \geq N_0$. Then for any $\gamma \in M_{p-1}(R)$ (c.f. 7.4.3) we have:*

$$A_{\gamma,n^*}(1)\left[t_1^{q\gamma-r^*(q-1)}\right]^{p^{n^*}} \in \mathcal{L}_{s_0-1}(v_0)A_{sep}+\sum_{1\leqslant s<s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep})+J_{s_0}.$$

Proof.

Lemma 7.5.4 (c.f. also n.7.11.5) gives

$$A_{\gamma,n^*}(1) = -\frac{1}{r^*}\mathcal{F}_{R,n^*}(\gamma,0)\operatorname{mod} J_{s_0+1},$$

where the elements $\mathcal{F}_{R,n^*}(\gamma,0)$ were defined in n.5. If $\gamma \geq v_0$, then

$$A_{\gamma,n^*}(1) \in \mathcal{L}_{R,N}^{(v_0)} \otimes k \operatorname{mod}(C_{s_0+1} \otimes k).$$

Therefore, $A_{\gamma,n^*}(1) \in \mathcal{L}_{s_0-1}(v_0) \otimes k$ for $\gamma \geq v_0$ (c.f. 7.7(a)).

If $\gamma < v_0$, then

$$t_1^{q\gamma-r^*(q-1)} \in t_1^{-r^*(p-1)p^{N_0}} O'_{tr}$$

(c.f. 7.4.3). Therefore,

$$A_{\gamma,n^*}(1)\left[t_1^{q\gamma-r^*(q-1)}\right]^{p^{n^*}} \in \left[t_1^{-r^*(p-1)p^{N_0}}\right]^{p^{n^*}} J_1(O_{sep}) \subset$$

$$\subset \sum_{1\leqslant s<s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}).$$

7.14.2. Lemma. *If $n^* \geq N_0$, then*

$$B_{\gamma,n^*}(1)\left[t_1^{q\gamma-r^*(q-1)}\right]^{p^{n^*}} \in \mathcal{L}_{s_0-1}(v_0)A_{sep}+$$

$$+\sum_{1\leqslant s_1,s_2<s_0}\left[t_1^{-r^*(p-s_1)p^{N_0}}\right]^{p^{n^*}}\left[t^{s_2\frac{r^*}{p}}\right]^{p^{n^*}} J_{s_1+s_2}(O_{sep})+J_{s_0}.$$

Proof.

The arguments of the proof of the proposition 7.12 give

$$C_{\gamma,n^*}^{(i)}\left[t_1^{q\gamma}\right]^{p^{n^*}} \in \mathcal{L}_{s_0-1}(v_0)A_{sep}+\sum_{1\leqslant s<s_0}\left[t^{s\frac{r^*}{p}}\right]^{p^{n^*}} J_s(O_{sep})+J_{s_0},$$

where $C_{\gamma,n^*}^{(i)}$, $i=1,2$, were defined in n.7.11.4.

From the Proposition 7.11.4, it follows that

$$A_{\gamma,n^*}(1) = \sum_{\substack{\gamma_1,\gamma_0,\gamma_2\\ \gamma_1+\gamma_0+\gamma_2=\gamma}} C_{\gamma_1,n^*}^{(1)}B_{\gamma_0,n^*}(1)C_{\gamma_2,n^*}^{(2)} \operatorname{mod} J_{s_0+1}.$$

The set $\{\gamma \mid B_{\gamma,n^*} \neq 0\}$ is finite. Now our Proposition can be proved by induction on γ from the above equality.

7.14.3. Lemma. *For any $1 \le m < p$ and $n^* \ge N_0$ we have:*

(a)

$$A_{\gamma,n^*}(m+1)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}} \in$$

$$\in \mathcal{L}_{s_0-1}(v_0)A_{sep} + \sum_{1\leqslant s<s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0};$$

(b)

$$B_{\gamma,n^*}(m)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}} \in$$

$$\in \mathcal{L}_{s_0-1}(v_0)A_{sep} + \sum_{1\leqslant s<s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0}.$$

Proof.

This statement can be proved by an induction on m.

Assume that this is proved for some m such that $m+1<p$. Then we have from Proposition 7.11.4 that

$$A_{\gamma,n^*}(m) = \sum_{\substack{\gamma_1,\gamma_0,\gamma_2\\ \gamma_1+\gamma_0+\gamma_2=\gamma}} C^{(1)}_{\gamma_1,n^*}B_{\gamma_0,n^*}(m)C^{(2)}_{\gamma_2,n^*} \bmod J_{s_0+1}.$$

By an induction on γ, as in the above Lemma, we obtain that

$$B_{\gamma,n^*}(m)\left[t_1^{q\gamma-mr^*(q-1)}\right]^{p^{n^*}} \in$$

$$\in \mathcal{L}_{s_0-1}(v_0)A_{sep} + \sum_{1\leqslant s_1,s_2<s_0}\left[t_1^{-r^*(p-s_1)p^{N_0}}\right]^{p^{n^*}}\left[t^{s_2\frac{r^*}{p}}\right]^{p^{n^*}} J_{s_1+s_2}(O_{sep}) + J_{s_0}.$$

Multiplying both sides of this expression by $\left[t_1^{-r^*(q-1)}\right]^{p^{n^*}}$ we obtain the formula (b) of our Proposition. The formula (a) follows now from Prop. 7.11.5.

7.14.4. Lemma. *Let $1 \le m < p$, $n^* \ge N_0$, then*

$$(m+1)A_{\gamma,n^*}(m+1)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}} \equiv -\gamma B_{\gamma,n^*}(m)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}}$$

$$\bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0+1}\right).$$

Proof. This follows from the above Lemma, relation of Proposition 7.11.5 and a trivial remark that, for any $\gamma > 0$, $A_{\gamma,n^*}(1), C^{(1)}_{\gamma,n^*}, C^{(2)}_{\gamma,n^*} \in J_1$.

7.14.5. Lemma. *If $1 \leq m < p$ and $n^* \geq N_0$, then*

$$A_{\gamma,n^*}(m)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}} \equiv B_{\gamma,n^*}(m)\left[t_1^{q\gamma-(m+1)r^*(q-1)}\right]^{p^{n^*}}$$

$$\mathrm{mod}\left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0+1}\right).$$

Proof.

This Lemma can be deduced from the relation of Proposition n.7.11.4 in the same way, as Lemma 7.14.4 was deduced from Proposition 7.11.5.

7.14.6. In order to finish the proof of our Proposition we remark that

$$A_{\gamma,n^*}\left[t_1^{q\gamma}\right]^{p^{n^*}} \equiv$$

$$\equiv \sum_{1\leqslant m<p} A_{\gamma,n^*}(m)\left[t_1^{q\gamma-mr^*(q-1)}\right]^{p^{n^*}} \ \mathrm{mod}\left[t_1^{q\gamma-pr^*(q-1)}\right]^{p^{n^*}} J_1(O_{sep}).$$

By the condition $\gamma \leq s_0 r^*$, we obtain:

$$q\gamma - pr^*(q-1) \leq q(p-1)r^* - pr^*(q-1) = -r^*(q-p) \leq -r^*(p-1)p^{N_0}$$

(we have: $q = p^N$ and $N > N_0$, c.f. n......).

Therefore, the above equivalence is valid modulo

$$\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0}\left[t_1^{-r^*(p-s)p^{N_0}}\right]^{p^{n^*}} J_s(O_{sep}) + J_{s_0+1}$$

and the above lemmas give the formula of our Proposition.

7.15. Proposition. *For any $\gamma \in M_{p-1}(R)$ we have:*

(a) if $\gamma > s_0 r^*$, then

$$A(\gamma)_0\left[t_1^{q\gamma}\right]^q \equiv -\frac{1}{r^*}\mathcal{F}_{R,N}(\gamma,0)\left[t_1^{q\gamma-r^*(q-1)}\right]^q$$

$$\mathrm{mod}\left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)}J_s(O_{sep}) + J_{s_0+1}\right);$$

(b) if $\gamma \leq s_0 r^*$, then

$$A(\gamma)_0\left[t_1^{q\gamma}\right]^q \equiv -\frac{1}{r^*}\mathcal{F}_{R,N}(\gamma,0)\sum_{m\geqslant 1}\frac{(-\gamma)^{m-1}}{m!}\left[t_1^{q\gamma-mr^*(q-1)}\right]^q$$

$$\mathrm{mod}\left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1\leqslant s\leqslant s_0} t^{-r^*(p-s)}J_s(O_{sep}) + J_{s_0+1}\right).$$

Proof.

This follows immediately from the above propositions 7.12-7.14 and the formula of the Prop. 7.11.3.

7.16. Let I be an ideal in $\mathcal{L}$ such that (c.f. n.7.10)

$$IA_{sep} \supset \mathcal{L}_{s_0-1}(v_0)J_1 + J_{s_0+1}$$

and let $X_1'' \in A_{sep}$ be the element from Proposition n.7.11.1.

Proposition. *The field of definition of $X_1'' \bmod IA_{sep}$ has upper ramification numbers $< v_0$ over K, if and only if $\mathcal{F}_{R,N}(\gamma, n) \in I \otimes k$ for $\gamma \geq 0$ and $0 \leq n < N$.*

Proof.

By the definition,

$$X_1''^{(q)} - X_1'' = \sum_{0 \leqslant m < N} A(s_0)_0^{(p^m)},$$

where (c.f. n.7.11.2)

$$\sum_{0 \leqslant m < N} A(s_0)_0^{(p^m)} = \sum_{\substack{\gamma \in \mathbb{Q} \\ 0 \leqslant m < N}} A(\gamma)_0^{p^m} \, [t_1^{q\gamma}]^{qp^m} \equiv$$

$$\equiv \sum_{\substack{0 \leqslant m < N \\ \gamma > s_0 r^*}} \mathcal{F}_{R,N}(\gamma, m) \left[t_1^{q\gamma - r^*(q-1)}\right]^{qp^m} + \sum_{\substack{0 \leqslant m < N \\ \gamma \leqslant s_0 r^*}} \mathcal{F}_{R,N}(\gamma, m) \sum_{m_1 \geqslant 1} \left[t_1^{q\gamma - m_1 r^*(q-1)}\right]^{qp^m}$$

$$\bmod \left(\mathcal{L}_{s_0-1}(v_0)J_1 + \sum_{1 \leqslant s \leqslant s_0} t^{-r^*(p-s)} J_s(O_{sep}) + J_{s_0+1} \right).$$

Let

$$\gamma_0(I) = \max\{ \gamma \mid \mathcal{F}_{R,N}(\gamma, m) \notin I \text{ for some } 0 \leq m < N \}.$$

If $\gamma_0 < v_0$, then $q\gamma_0 - r^*(q-1) < 0$ and $X_1'' \bmod (IA_{sep}$ defines the trivial extension of K_{tr}'.

If $\gamma_0 \geq v_0$, then $q\gamma_0 - r^*(q-1) > 0$ (c.f. n.7.4.3) and the field of definition of $X_1'' \bmod (IA_{sep}$, which we denote by $L''(I)$ has the largest upper ramification number equal to γ_0. Indeed, it follows from n.6.3 that $v(L''(I)/K') = q\gamma_0 - r^*(q-1)$, hence

$$v(L''(I)/K) = \frac{q\gamma_0 - r^*(q-1) - r^*}{q} + r^* = \gamma_0.$$

Therefore,

$$I \supset \mathcal{L}_{s_0}(v_0) \Leftrightarrow \mathcal{F}_{R,N}(\gamma, m) \in I \otimes k \text{ for all } \gamma_0 \geq v_0.$$

This gives the inductive assumption 7.7(a) for $s^* = s_0 + 1$. All other assumptions are the easy consequences of the above formulae.

REFERENCES

[A1] V.A.Abrashkin, *The Galois modules of the period p group schemes over the ring of Witt vectors*, Math. USSR Izv. **31** (1988).

[A2] V.A.Abrashkin, *Group schemes over a discrete valuation ring with small ramification*, Leningrad Math. J. **1** (1990), no. 1, 57-97.

[A3] V.A.Abrashkin, *Modular representations of the Galois group of a local field and a generalisation of the Shafarevich conjecture*, Math. USSR Izv. **35** (1990), no. 3, 469-518.

[A4] V.A.Abrashkin, *Ramification in étale cohomology*, Invent. Math. **101** (1990), 631-640.

[B] N.Bourbaki, *Lie groups and Lie algebras*, Part I: Chapters 1-3, Hermann, 1975.

[De] P.Deligne, *Les corps locaux de caracteristique p, limites de corps locaux de caracteristique 0*, Représentations des groupes réductifs. (J.-N. Bernstein etc., eds.), Collection: Travaux en cours, Hermann, Paris, 1984.

[Di] B.Ditters, *Groupes formels*, Cours 3e cycle 1973-1974. Preprint Universite Paris XI, 149-75.42.

[Fa] G.Faltings, *Crystalline Cohomology and p-adic Galois representations*, Algebraic Analysis, Geometry, and Number Theory (Jun-Ichi Igusa, eds.), Proceed. of the JAMI Inaugural Conference, John Hopkins University Press.

[F1] J.-M.Fontaine, *Il n'y a pas de varieté abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), 515-538.

[F2] J.-M.Fontaine, *Letter to W. Messing, 15 jan.* (1986).

[F3] J.-M. Fontaine, *Representations 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.

[F-M] J.-M.Fontaine and W.Messing, *p-adic periods and p-adic étale cohomology*, Contemp. Math. **67** (1987), 179-207.

[Go] N.L.Gordeev, *Infinity of the number of relations in the Galois group of maximal p-extension with bounded ramification of a local field (Russian)*, Dokl.Akad.Nauk SSSR **233** (1977), no. 6, 1031-1034.

[In1] E.Inaba, *On matrix equations for Galois extensions of fields with characteristic p*, Natur.Sci. Rep. Ochanomizu Univ. **12** (1961), 26-36.

[In2] E.Inaba, *On generalized Artin-Schreier equations*, Natur.Sci. Rep. Ochanomizu Univ. **13** (1962), 1-13.

[In3] E.Inaba, *Normal form of generalized Artin-Schreier equations*, Natur.Sci. Rep. Ochanomizu Univ. **14** (1963), 1-15.

[J-W] U.Jannssen and K.Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkorper*, Invent. math. **70** (1982), 71-98.

[Jac] A.V.Jakovlev, *The Galois group of the algebraic closure of a local field*, Math. USSR-Izv. **2** (1968), 1231-1269.

[Ma] E.Maus, *Relationen in Verzweigungsgruppen*, J.Reine Angew.Math. **258** (1973), 23-50.

[R] M. Raynaud, *Schemas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241-280.

[Se1] J.-P.Serre, *Sur les groupes de Galois attaches aux groupes p-divisibles*, Proc.Conf.Local Fields (Driebergen,1966), Springer, Berlin, 1967, pp. 118-131.

[Se2] J.-P.Serre, *Cohomologie Galoisienne*, Lecture Notes on Math.,Springer-Verlag, Berlin-Heidelberg-New York, vol. 5, 1973.

[Se3] J.-P.Serre, *Local fields*, (Graduate texts in math.; 67). Springer-Verlag, Berlin-Heidelberg-New York. Translation of Corps Locaux, 1979.

[Wtt] E. Witt, *Zyclische Korper und Algebren der Charakteristik p vom Grad* p^n, J.Reine Angew. Math **176** (1936), 126-140.

[Wnt] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. Sci. Ecole Norm. Sup. **16** (1983), 59-89.