A STRONG PROPERTY OF RAMIFICATION FILTRATION

Victor A. Abrashkin

Under some natural assumptions about the structure of a finite extension K of $\mathbb{Q}_p$ we prove that it can be uniquely recovered from its Galois group with filtration by higher ramification subgroups.
Bibl. — 9 issues.

0. Introduction.

Throught all this paper p is a prime number, K is a finite extension of the p-adic field $\mathbb{Q}_p$, $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$, where $\bar{K}$ is some fixed algebraic closure of K, k is the residue field and e_K is the absolute ramification index of K. We also use permanently the notation $\mathbb{Z}^+(p)$ for the set of natural numbers prime to p.

0.1. The group theoretic structure of the Galois group Γ_K depends only on simplest invariants of the field K and was completely described in [J-W]. This description shows that the field K can not be recovered by its Galois group (in the case of global fields the situation is completely different by the Neukirch-Uchida-Iwasawa-Ikeda Theorem, cf. [Po] for this and another results related to Grothendieck's anabelian philosophy). Consider an additional structure on Γ_K given by decreasing filtration of its ramification subgroups in upper numbering $\{\Gamma_K^{(v)}\}_{v\geqslant -1}$ (cf. [Se] for the definition). We note that $\Gamma_K^{(-1)} = \Gamma_K$; for $-1 < v \leqslant 0$, $\Gamma_K^{(v)} = \mathrm{Gal}(\bar{K}/K_{\mathrm{ur}})$; the group $\Gamma^{(0+)} := \bigcup_{v>0} \Gamma_K^{(v)}$ coincides with $\mathrm{Gal}(\bar{K}/K_{\mathrm{tr}})$ (here K_{ur} (resp., K_{tr}) is the maximal unramified (resp., tamely ramified) extension of K in $\bar{K}$), and all rational positive numbers appear as jumps of this filtration.

The following questions appear very naturally:

a) Is the field K uniquely determined by the filtered group $\{\Gamma_K^{(v)}\}_{v\geqslant -1}$?

b) Choose an algebraic closure $\bar{\mathbb{Q}}_p$ and consider two finite extensions K_1 and K_2 in $\bar{\mathbb{Q}}_p$. Does any compatible with ramification filtrations isomorphism from Γ_{K_1} to Γ_{K_2} comes from an inner automorphism of $\Gamma_{\mathbb{Q}_p}$?

c) Let $\mathcal{K} = k((t))$, where k is a finite field. Does any compatible with ramification filtration automorphism of the Galois group $\mathcal{G}_{\mathcal{K}} = \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})$ comes from conjugation by an automorphism of $\mathcal{K}_{\mathrm{sep}}$?

0.2. The above questions seem to be very difficult to answer, because our knowledge of ramification filtration is far from to be complete. We are going to apply

The author had a nice opportunity to work on this subject during his stay at the Sydney University (the end of 1997) and at the MPI, Bonn (the spring of 1998), and expresses his gratitude to these organisations for hospitality. He is also very grateful to Dr. K.F.Lai (Sydney University) for helpful and stimulating discussions.

our recent results about this filtration from [Ab1,2] to study the following slightly modified question.

What properties of the field K can be recovered from the structure of the filtered group $\{\Gamma_K^{(v)}/\Gamma_K^{(a)}\}_{-1\leqslant v\leqslant a}$, where $a>0$ is some fixed rational number?

In the paper [De] it was shown that the group $\Gamma_K/\Gamma_K^{(a)}$ together with its ramification filtration depends roughly speaking only on the structure of the artinian algebra $O_K \bmod \pi_K^{a+1}$, where O_K is the valuation ring of K and π_K is its uniformising element.

So, the field K can not be reconstructed completely in the general case by the knowledge only of some segment of the ramification filtration. Nevertheless, one can use the structure of $O_K \bmod \pi_K^{a+1}$ to recover the field K under some natural additional assumptions. Namely, let E be a complete subfield of K. Define the rational positive number

$$v(K/E)=\max\{v \mid \Gamma_E^{(v)} \quad \text{acts nontrivially on} \quad K\}.$$

We note that such number exists because of the left-continuity property of ramification filtration. If we assume the field E to be given, then Krasner's lemma implies that the extension K/E is uniquely determined by the O_E-algebra $O_K \bmod \pi_E^{v(K/E)+1+\varepsilon}$, where ε is any positive number (for any $b\in\mathbb{R}$, the ideal (π_E^b) is the ideal of elements $\alpha\in K$ having the valuation $v(\alpha)\geqslant bv(\pi_E)$). We apply this argument below to recover uniquely the field K as an extension of the cyclotomic field $\mathbb{Q}_p(\zeta_M)$, where ζ_M is a primitive root of unity of degree p^M, $M\in\mathbb{N}$, in the case when this extension is not "very wildly" ramified.

0.3. In fact, the main result of this paper deals with more simple filtered group $\{\Gamma_K(p)^{(v)}/\Gamma_K(p)^{(a)}\}_{-1\leqslant v\leqslant a}$, where $\Gamma_K(p)$ is the Galois group of the maximal p-extension $K(p)$ of K in $\bar{K}$. The following properties show, nevertheless, that this quotient still has sufficiently rich structure:

a) the group $\Gamma_K(p)/\Gamma_K(p)^{(a)}$ has finitely many generators but infinitely many relations, cf. [Go] (also [Ma]);

b) any finitely generated, closed but not open subgroup of $\Gamma_K(p)/\Gamma_K(p)^{(a)}$ is a free pro-p-group, cf. [Ab3]. Roughly speaking, this group does not have "simple" relations, i.e. any relation can not be expressed in terms of any proper subset of any minimal system of generators. In particular, it does not have torsion and nontrivially commuting elements.

0.4. In order to formulate our main result, assume that $p\geqslant 5$, a primitive root ζ_M of degree p^M, where $M\in\mathbb{N}$, belongs to K, and the degree $f_K=[k:\mathbb{F}_p]$ of the residue field k of K is sufficiently large, or more precisely, $f_K\geqslant 2\log_p(p^2v_K)$, where $v_K=p^{M+1}e_K/(p-1)$.

Theorem. *Under the above assumptions let $a_K=e_K\,(p/(p-1)+M)$ and assume that for a finite extension K' of $\mathbb{Q}_p$ in $\bar{K}$ there exists a compatible with ramification filtration group isomorphism*

$$G:\Gamma_K(p)/\Gamma_K(p)^{(a_K)}\longrightarrow \Gamma_{K'}(p)/\Gamma_{K'}(p)^{(a_K)}.$$

Then $\zeta_M\in K'$, $e_{K'}=e_K$ and for some $\phi\in\mathrm{Gal}(\mathbb{Q}_p(\zeta_M)/\mathbb{Q}_p)$, there exists ϕ-linear isomorphism of $\mathbb{Z}_p[\zeta_M]$-algebras

$$O_K \bmod p^{1/(p-1)}\simeq O_{K'} \bmod p^{1/(p-1)}.$$

The existence of an isomorphism of the above two $\mathbb{Z}_p[\zeta_M]$-algebras is equivalent to the fact, that truncated decompositions of primitive roots of unity $\zeta_M\in K$ and $\phi(\zeta_M)\in K'$ in powers of some uniformizing elements $\pi\in K$ and $\pi'\in K'$ modulo $p^{1/(p-1)}$ have "the same " coefficients under some isomorphism of residue fields.

This result can be considered as an evidence to believe that the answer to the question a) of n.0.1 should be positive. It becomes clear from the proof of the theorem that the condition for an automorphism of the group Γ_K (and the group $\mathcal{G}_{\mathcal{K}}$ in the finite characteristics case) to be compatible with ramification filtration is very restrictive. This can be considered as an argument for expecting the positive answer to the questions b) and c) of n.0.1.

0.5. As we already have mentioned in n.0.2, the field K can be recovered from the filtered group $\{\Gamma_K(p)^{(v)}/\Gamma_K(p)^{(a_K)}\}_{-1\leqslant v\leqslant a_K}$ under some additional assumptions. We apply this argument for the following statement.

Corollary. *If $v(K'/\mathbb{Q}_p(\zeta_M))<p^{M-1}-1$, then such field K' is unique up to isomorphism. In particular, if $v(K/\mathbb{Q}_p(\zeta_M))<p^{M-1}-1$, then $K\simeq K'$.*

This follows immediately from above mentioned Krasner's lemma (cf. n.0.2). Indeed, we can take $E=\mathbb{Q}_p(\zeta_M)$, $\pi_E=\zeta_M-1$. Then it is sufficient to note that for some $\varepsilon>0$, there is the following equality of ideals in O_K

$$\left(p^{1/(p-1)}\right)=\left(\pi_E^{p^{M-1}}\right)=\left(\pi^{v(K/\mathbb{Q}_p(\zeta_M))+1+\varepsilon}\right).$$

Denote by $\mathcal{A}_M$ the set of finite extensions K of $\mathbb{Q}_p(\zeta_M)$ in $\bar{K}$ such that $v(K/\mathbb{Q}_p(\zeta_M))<p^{M-1}-1$. Then elementary calculations with Herbrandt's function give that $K\in\mathcal{A}_M$ iff $K=K_1\mathbb{Q}_p(\zeta_M)$, where $[K_1:\mathbb{Q}_p]<\infty$ and $v(K_1/\mathbb{Q}_p)<M-1$.

This alows us to reformulate the main result of this paper in the following form.

Corollary. *If $p\geqslant 5$ and $K\in\mathcal{A}_M$ has sufficiently large residue field, then it can be uniquely recovered from the filtered group $\{\Gamma_K(p)/\Gamma_K(p)^{(a_K)}\}_{-1\leqslant v\leqslant a_K}$.*

0.6. We outline briefly the basic ideas and constructions used in the proof of our theorem. In n.4 we construct the fundamental exact sequence to express the group $\Gamma_K(p)/\Gamma_K(p)^{(a_K)}$ as an extension of the cyclic group $\mathrm{Gal}(K(\pi_K^{1/p^M})/K)\simeq\mathbb{Z}/p^M\mathbb{Z}$ by the quotient $\mathcal{G}(p)/\mathcal{G}(p)^{(v_K)}$, where $\mathcal{G}(p)$ is the Galois group of the maximal p-extension of a complete discrete valuation field $\mathcal{K}=k((t))$ of characteristic p. This construction is a suitable application of the Fontaine-Wintenberger field-of-norms functor, [Wi].

In Section 5 we prove that the isomorphism G relates fundamental exact sequences for the fields K and K'. This gives automorphism of the group $\mathcal{G}(p)/\mathcal{G}(p)^{(v_K)}$, which is compatible with ramification filtration and relates actions of $\mathbb{Z}/p^M\mathbb{Z}$ by conjugation on this group coming from the fields K and K'.

In Section 3 we use our general result about the structure of ramification filtration modulo commutators of order $\geqslant p$ in the characteristic p case, [Ab1,2]. This description provides us with generators of ramification subgroups explicitly given in terms of so-called special basises of the W-module $\mathcal{G}(p)^{\mathrm{ab}}\otimes W$ (W is the Witt vectors ring with coefficients in k). In fact, we apply this description to a considerably more simple group $\bar{\mathcal{G}}/\bar{\mathcal{G}}^{(v_K)}$, where $\bar{\mathcal{G}}=\mathcal{G}(p)/\mathcal{G}(p)^{p^3}C_3(\mathcal{G}(p))$ and $C_3(\mathcal{G}(p))$ is the subgroup of commutators of order $\geqslant 3$, and use only the "modulo t^{v_K}"-part of the special basis. The main lemma of n.3 states that any compatible with ramification filtration automorphism of the group $\bar{\mathcal{G}}$ "almost " preserves the "modulo $t^{v_K/p}$"-part of special basises.

On the other hand, the actions of $\mathbb{Z}/p^M\mathbb{Z}$ on the quotient $\left(\bar{\mathcal{G}}/\bar{\mathcal{G}}^p\right)^{\mathrm{ab}}$ of the group $\bar{\mathcal{G}}$ coming from the fundamental exact sequence related to the field K (resp., K') can be expressed in terms of expansions of some roots of degree p^M from unity in power series in uniformiser π_K (resp., $\pi_{K'}$) by the use of special basises. This alows us to relate in Section 5 these expansions modulo $p^{1/(p-1)}$, what gives finally the proof of our theorem.

1. Preliminaries: special basises.

In this section $\mathcal{K}$ is a complete discrete valuation field of characteristic p with finite residue field $k \simeq \mathbb{F}_{p^{N_0}}$. We assume that a separable closure $\mathcal{K}_{\mathrm{sep}}$ of $\mathcal{K}$ is chosen and set $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})$.

1.1. Consider the p-completion $\hat{\mathcal{K}}^* = \varprojlim \mathcal{K}^*/\mathcal{K}^{*p^n}$ of the multiplicative group $\mathcal{K}^*$ with its natural $\mathbb{Z}_p$-algebra structure. Fix a uniformising element t of the field $\mathcal{K}$ and consider the $\mathbb{Z}_p$-algebra isomorphism

$$\chi_t : \hat{\mathcal{K}}^* \longrightarrow \mathbb{Z}_p \times \prod_{a \in \mathbb{Z}^+(p)} W_a,$$

where for all $a \in \mathbb{Z}^+(p)$, $W_a = W$ is the $\mathbb{Z}_p$-algebra of Witt vectors with coefficients in k. The isomorphism χ_t is induced by the decomposition of any element $\alpha \in \mathcal{K}^*$ in the form

$$\alpha = t^{a_0(\alpha)} \prod_{(a,p)=1} E(w_a(\alpha), t^a),$$

where $a_0(\alpha) \in \mathbb{Z}$, $w_a(\alpha) \in W$ for all $(a,p) = 1$, and for any $w \in W$,

$$E(w, X) = \exp\left(wX + \dots + \sigma^n(w)X^{p^n}/p^n + \dots\right) \in W[[X]]$$

(as usually, σ is the Frobenius morphism of Witt vectors).

Consider extension of scalars of χ_t

$$\chi_t \otimes W : \hat{\mathcal{K}}^* \otimes W \longrightarrow W_0 \times \prod_{\substack{(a,p)=1 \\ n \in \mathbb{Z} \bmod N_0}} W_{an}.$$

Here $W_0 = W$ and the W-algebras W_{an} consist of elements of W with the W-algebra structure coming from the morphism $\sigma^{-n} : W \longrightarrow W$. The action of σ on scalars gives σ-linear automorphism of $\hat{\mathcal{K}}^* \otimes W$. We shall denote this morphism also by σ. We note that $(\hat{\mathcal{K}}^* \otimes W)|_{\sigma=\mathrm{id}} = \hat{\mathcal{K}}^*$.

The algebras W_0 and W_{an} have standard generators D_0 and D_{an} coming from $1 \in W$. The system

$$\mathcal{D}(t) = \{D_{an} \mid (a,p) = 1, n \in \mathbb{Z} \bmod N_0\} \cup \{D_0\}$$

gives a topological basis of the W-algebra $\hat{\mathcal{K}}^* \otimes W$. This basis depends only on the choice of uniformiser in $\mathcal{K}$. We note that σ acts on its elements D_{an} by the shift $\sigma : D_{an} \mapsto D_{a,n+1}$, and $\sigma(D_0) = D_0$, i.e. $D_0 \in \hat{\mathcal{K}}^*$. On the other hand, if fr_t is an automorphism of the field $\mathcal{K}$ such that $\mathrm{fr}_t(t)=t$ and $\mathrm{fr}_t|_k=\sigma$, then $\mathrm{fr}_t(D_{an})=D_{a,n-1}$ for all $a\in\mathbb{Z}^+(p)$ and $n\in\mathbb{Z}\,\mathrm{mod}\,N_0$.

If we take elements from $\mathcal{D}(t)$ modulo p, we obtain a basis of the k-module $\mathcal{K}^*/\mathcal{K}^{*p}\otimes k$. The basises $\mathcal{D}(t)$ and $\mathcal{D}(t)\,\mathrm{mod}\,p$ will be called special basises.

1.2. Consider the quotient $\mathcal{M}=\mathcal{G}/\mathcal{G}^pC_2(\mathcal{G})$ as a profinite $\mathbb{F}_p$-module, and introduce $\mathbb{F}_p$-modules $\mathcal{M}_k=\mathcal{M}\hat{\otimes}k$, $\mathcal{M}_{\mathcal{K}}=\mathcal{M}\hat{\otimes}\mathcal{K}$, and $\mathcal{M}_{\mathrm{sep}}=\mathcal{M}\hat{\otimes}\mathcal{K}_{\mathrm{sep}}$. All these modules have the natural action of the Frobenius morphism coming from extension of scalars. We shall denote this action also by σ. The module $\mathcal{M}_{\mathrm{sep}}$ has also natural action of the Galois group $\mathcal{G}$.

The Artin-Schreier theory gives the identification $\mathcal{M}=\mathrm{Hom}\,(\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K},\mathbb{F}_p)$. Its equivalent version can be given as follows. If $\tilde{e}\in\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$, take its lifting $e\in\mathcal{M}_{\mathcal{K}}$ with respect to the natural projection to $\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$, and take $F\in\mathcal{M}_{\mathrm{sep}}$ such that $\sigma F-F=e$. Then for any $\tau\in\mathcal{G}$, the correspondence

$$\tau\mapsto\tau F-F\in\mathcal{M}_{\mathrm{sep}}|_{\sigma=\mathrm{id}}=\mathcal{M}$$

gives an element of $\mathrm{Hom}(\mathcal{G},\mathcal{M})$. So, we have the map

$$\psi_1:\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}\longrightarrow\mathrm{Hom}(\mathcal{G},\mathcal{M})$$

and this map is isomorphism.

We note that

$$\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}=\mathrm{End}_{\mathbb{F}_p}(\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K})$$

and if $\bar{e}\in\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$ corresponds to the identity endomorphism of $\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$, then $\psi_1(\bar{e})$ is nothing but the natural projection $\pi:\mathcal{G}\longrightarrow\mathcal{M}$.

1.3. Take an uniformiser t of $\mathcal{K}$ and an element $\alpha_0\in k$ such that $\mathrm{Tr}_{k/\mathbb{F}_p}\alpha_0=1$. Then the natural projection from $\mathcal{K}$ to $\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$ has the unique section with values in the $\mathbb{F}_p$-submodule $\mathbb{F}_p\alpha_0\oplus(\oplus_{a\in\mathbb{Z}^+(p)}t^{-a}k)$ of $\mathcal{K}$. We use this section to obtain the lifting $e_{\alpha_0,t}\in\mathcal{M}_{\mathcal{K}}$ of the element $\bar{e}\in\mathcal{M}\otimes\mathcal{K}/(\sigma-\mathrm{id})\mathcal{K}$ defined in above n.1.2.

Lemma. *Under the class field theory identification $\mathcal{M}=\mathcal{K}^*/\mathcal{K}^{*p}$, we have*

$$e_{\alpha_0,t_0}=\alpha_0D_0+\sum_{a\in\mathbb{Z}^+(p)}t^{-a}D_{a0},$$

where D_0 and D_{a0} for all $a\in\mathbb{Z}^+(p)$, are elements from the special basis $\mathcal{D}(t)\,\mathrm{mod}\,p$, cf. n.1.1.

The proof is an easy application of the Artin-Schreier explicit reciprocity law.

1.4. It can be verified easily that the condition $\mathrm{Tr}_{k/\mathbb{F}_p}\alpha_0=1$ implies that D_0 induces the Frobenius automorphism on the maximal unramified extension $\mathcal{K}_{ur}^{(1)}/\mathcal{K}$ inside $\mathcal{K}^{(1)}=\mathcal{K}_{\mathrm{sep}}^{\mathcal{G}^pC_2(\mathcal{G})}$. Set $\mathcal{M}^{(1)}=\mathrm{Gal}(\mathcal{K}^{(1)}/\mathcal{K}_{ur}^{(1)})\subset\mathcal{M}=\mathrm{Gal}(\mathcal{K}^{(1)}/\mathcal{K})$. Then $\mathcal{M}^{(1)}$ is the inertia subgroup of $\mathcal{M}$, and the elements of the set $\mathcal{D}^{(1)}(t)\,\mathrm{mod}\,p$, where

$$\mathcal{D}^{(1)}(t):=\{D_{an}\mid(a,p)=1,n\in\mathbb{Z}\,\mathrm{mod}\,N_0\}=\mathcal{D}(t)\setminus\{D_0\},$$

give a special basis of the k-submodule $\mathcal{M}_k^{(1)} := \mathcal{M}^{(1)} \otimes k$ of $\mathcal{M}_k$. We agree to use also the notation D_{an} for elements of the set $\mathcal{D}^{(1)}(t) \bmod p$.

If t' is another uniformiser of the field $\mathcal{K}$, then the elements of

$$\mathcal{D}^{(1)}(t') \bmod p = \{D'_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\},$$

give another special k-basis of $\mathcal{M}_k^{(1)}$. Therefore, for $a \in \mathbb{Z}^+(p)$ we have

$$D'_{a0} = \sum \alpha_{abm} D_{bm},$$

where the sum is taken for $b \in \mathbb{Z}^+(p)$ and $m \in \mathbb{Z} \bmod N_0$, and all coefficients α_{abm} belong to k. It can be immediately seen from definitions that $\alpha_{abm} = 0$ if $b < a$. We also note that , if $a \in \mathbb{Z}^+(p)$, $n \in \mathbb{Z} \bmod N_0$, and

$$D'_{an} = \sum_{\substack{(b,p)=1 \\ m \in \mathbb{Z} \bmod N_0}} \alpha_{anbm} D_{bm}$$

with all $\alpha_{anbm} \in k$, then $\alpha_{anbm} = \sigma^n(\alpha_{a,b,m-n})$. In particular, $\alpha_{anbm} = 0$ for $b < a$.

1.5. We need more precise information concerning the relation between elements of two different special basises of $\mathcal{M}_k^{(1)}$. Lemma of n.1.3 and the formalism of Artin-Schreier theory from n.1.2 imply the following property.

Lemma. *If t and t' are uniformising elements of $\mathcal{K}$, then the elements of special basises $\mathcal{D}^{(1)}(t) \bmod p$ and $\mathcal{D}^{(1)}(t') \bmod p$ are related by the equality*

$$\sum_{a \in \mathbb{Z}^+(p)} t^{-a} D_{a0} \equiv \sum_{a \in \mathbb{Z}^+(p)} t'^{-a} D'_{a0} \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}}.$$

For $a \in \mathbb{N}$, denote by $\mathcal{M}^{(a)}$ the submodule of $\mathcal{M}$, which consists of elements coming from principal units congruent to unity modulo a^{th} power of the maximal ideal of the valuation ring $O_{\mathcal{K}}$ of the field $\mathcal{K}$. Set $\mathcal{M}_k^{(a)} = \mathcal{M}^{(a)} \otimes k$, and apply the above lemma to prove the following proposition.

Proposition. *For any $a \in \mathbb{Z}^+(p)$, we have:*
a) *if $t' \equiv \alpha t \bmod t^2$, where $\alpha \in k$, then*

$$D'_{a0} \equiv \alpha^a D_{a0} \bmod \mathcal{M}_k^{(a+1)};$$

b) *let $t' \equiv t + \alpha t^{b+1} \bmod t^{b+2}$, where $b \geqslant 1$ and $\alpha \in k$; then for $a \not\equiv -b \bmod p$,*

$$D'_{a0} \equiv D_{a0} + (a+b)\alpha D_{a+b,0} \bmod \mathcal{M}_k^{(a+b+1)};$$

and for $a \equiv -b \bmod p$,

$$D'_{a0} \equiv D_{a0} \bmod \mathcal{M}_k^{(a+b+1)}.$$

Proof. From the congruence $t' \equiv \alpha t \bmod t^2$ it follows that for any $a \in \mathbb{Z}^+(p)$ and some coefficients $\beta_{ab} \in k$ defined for $1 \leqslant b < a$, we have

$$t'^{-a} \equiv \alpha^{-a} t^{-a} + \sum_{1 \leqslant b < a} \beta_{ab} t^{-b} \bmod O_{\mathcal{K}}.$$

Then

$$\sum_{a\in\mathbb{Z}^+(p)} t'^{-a}D'_{a0} \equiv \sum_{a\in\mathbb{Z}^+(p)} \alpha^{-a}t^{-a}D'_{a0} + \sum_{\substack{a\in\mathbb{Z}^+(p)\\ 1\leqslant b<a}} \beta_{ab}t^{-b}D'_{a0} \equiv$$

$$\sum_{a\in\mathbb{Z}^+(p)} t^{-a}\left(\alpha^{-a}D'_{a0}+\sum\sigma^{-s}(\beta_{a',ap^s})D'_{a',-s}\right)\operatorname{mod}(\sigma-\mathrm{id})\mathcal{M}_{\mathcal{K}}+\mathcal{M}\otimes O_{\mathcal{K}},$$

where the last sum is taken for $a'\in\mathbb{Z}^+(p)$ and $s\in\mathbb{Z}_{\geqslant 0}$, such that $a'>ap^s$. This gives $D_{a0}\equiv\alpha^{-a}D'_{a0}\operatorname{mod}\mathcal{M}_k^{(a+1)}$. The part a) is proved.

In order to prove the part b) we note that for some $\beta_{ac}\in k$, where $a\in\mathbb{Z}^+(p)$ and $1\leqslant c<a-b$, we have

$$t'^{-a}\equiv t^{-a}-a\alpha t^{-a+b}+\sum_{1\leqslant c<a-b}\beta_{ac}t^{-c}\operatorname{mod}O_{\mathcal{K}},$$

and the proof can be finished similarly as in the previous case.

1.6. Consider a k-basis $\{C_{an}\mid a\in\mathbb{Z}^+(p), n\in\mathbb{Z}\operatorname{mod}N_0\}$ of $\mathcal{M}_k^{(1)}$ satisfying for all $a\in\mathbb{Z}^+(p)$ and $n\in\mathbb{Z}\operatorname{mod}N_0$ the following conditions:
a) $\sigma C_{an}=C_{a,n+1}$;
b) the elements of the set $\{C_{bm}\mid b\in\mathbb{Z}^+(p), b\geqslant a, m\in\mathbb{Z}\operatorname{mod}N_0\}$ generate the k-module $\mathcal{M}_k^{(a)}$.

Proposition. *If the system of elements $\{C_{an}\in\mathcal{M}_k^{(1)}\mid a\in\mathbb{Z}^+(p), n\in\mathbb{Z}\operatorname{mod}N_0\}$ satisfies the above conditions a) and b), then there exists $n_0\in\mathbb{Z}\operatorname{mod}N_0$ and a special basis $\{D_{an}\mid a\in\mathbb{Z}^+(p), n\in\mathbb{Z}\operatorname{mod}N_0\}$ such that if*

$$\sigma^{n_0}C_{a0}=\sum_{\substack{b\in\mathbb{Z}^+(p)\\ m\in\mathbb{Z}\operatorname{mod}N_0}}\alpha_{abm}D_{bm},$$

where all coefficients α_{abm} belong to k, then
1) *$\alpha_{110}=1$;*
2) *for all $b\in\mathbb{Z}^+(p)$ and $b>1$, we have $\alpha_{1b0}=0$;*
3) *for all $b\in\mathbb{N}$ such that $b\equiv 1\operatorname{mod}p$, we have $\alpha_{2b0}=0$.*

Proof. Choose a uniformiser t of the field $\mathcal{K}$, consider corresponding special basis

$$\mathcal{D}^{(1)}(t)\operatorname{mod}p=\{D_{an}\mid a\in\mathbb{Z}^+(p), n\in\mathbb{Z}\operatorname{mod}N_0\},$$

and set

$$C_{10}=\sum_{b,m}\alpha_{1bm}D_{bm},\qquad C_{20}=\sum_{b,m}\alpha_{2bm}D_{bm}.$$

By changing, if necessary, the system C_{an} to the system $\sigma^{n_0}C_{an}$ for some $n_0\in\mathbb{Z}\operatorname{mod}N_0$, we can assume that $\alpha_{110}\neq 0$.

Now we reformulate our proposition in the following form

there exists a special basis $\mathcal{D}^{(1)}(t)\operatorname{mod}p$ such that $\alpha_{110}=1$ and for all natural numbers $n>1$, we have $\alpha_{1n0}=0$ if $n\in\mathbb{Z}^+(p)$, and $\alpha_{2,n+1,0}=0$ if $n\equiv 0\operatorname{mod}p$.

We prove it by induction on n.

If $n = 1$, then we apply the part a) of Proposition n.1.5 to make a suitable change of the uniformiser t modulo t^2 to obtain the coefficient $\alpha_{110} = 1$ in the new special basis.

Now we assume that if $n \geqslant 2$, then $\alpha_{1b0} = 0$ for all $1 < b < n$, $b \in \mathbb{Z}^+(p)$, and $\alpha_{2b0} = 0$ for all $b \equiv 1 \bmod p$, $b < n+1$.

If $n \not\equiv 0 \bmod p$, then by the part b) of the proposition of n.1.5, we can chose a new uniformiser $t' = t + \alpha t^n$ for a suitable $\alpha \in k$, to annihilate α_{1n0}. We note that this procedure does not disturb the coefficients α_{2b0} for all $2 \leqslant b \leqslant n$.

If $n \equiv 0 \bmod p$, then we apply again the above proposition for a suitable uniformiser $t' = t + \alpha t^n$, $\alpha \in k$, to annihilate $\alpha_{2,n+1,0}$. Again this operation does not disturb the coefficients α_{1b0} and α_{2b0} for $1 \leqslant b \leqslant n$.

1.7. Consider the group $\operatorname{Aut}\mathcal{K}$ of all continuous automorphisms of the field $\mathcal{K}$. If $\phi \in \operatorname{Aut}\mathcal{K}$, consider $\hat{\phi} \in \operatorname{Aut}\mathcal{K}_{\mathrm{sep}}$ such that $\hat{\phi}|_{\mathcal{K}} = \phi$ and for $\tau \in \mathcal{G}$, set $\phi * \tau = \hat{\phi}^{-1}\tau\hat{\phi}$. This induces some action of $\hat{\phi}$ on $\mathcal{M}$, which does not depend on the choice of lifting $\hat{\phi}$ of ϕ. So, we can set $\hat{\phi} * m = \phi * m$ for any $m \in \mathcal{M}$. We use the same symbol for extension of scalars of this action to $\mathcal{M}_k$.

Denote by $\operatorname{Aut}^1\mathcal{K}$ the sugroup of $\operatorname{Aut}(\mathcal{K})$ consisting of automorphisms inducing identity on the residue field k of $\mathcal{K}$. Take uniformising element t of the field $\mathcal{K}$, and consider corresponding special basis of $\mathcal{M}_k^{(1)}$

$$\mathcal{D}^{(1)}(t) \bmod p = \{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\}.$$

Proposition 1. *If $\phi \in \operatorname{Aut}^1(\mathcal{K})$, then*

$$\sum_{a \in \mathbb{Z}^+(p)} \phi^{-1}(t)^{-a} D_{a0} \equiv \sum_{a \in \mathbb{Z}^+(p)} t^{-a}(\phi * D_{a0}) \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}}.$$

Proof. Take $F \in \mathcal{M}_{\mathrm{sep}}$ such that

$$\sigma F - F = \sum_{a \in \mathbb{Z}^+(p)} t^{-a} D_{a0} + \alpha_0 D_0,$$

then $\tau F - F = \pi(\tau)$, where $\tau \in \mathcal{G}$ and $\pi : \mathcal{G} \longrightarrow \mathcal{M}$ is the natural projection.

Take a lifting $\hat{\phi} \in \operatorname{Aut}^1\mathcal{K}_{\mathrm{sep}}$ and set $F_1 = \hat{\phi}^{-1}(F)$. Then

$$\sigma F_1 - F_1 = \sum_{a \in \mathbb{Z}^+(p)} \phi^{-1}(t)^{-a} D_{a0} + \alpha_0 D_0.$$

If $\tau \in \mathcal{G}$, then

$$\tau F_1 - F_1 = \hat{\phi}^{-1}\left((\hat{\phi} * \tau)F - F\right) = (\hat{\phi} * \tau)F - F = \pi(\hat{\phi} * \tau) = \phi * \pi(\tau).$$

But the homomorphism $\tau \mapsto \phi * \pi(\tau)$ can be obtained by the correspondence $\tau \mapsto \tau F_2 - F_2$, where

$$\sigma F_2 - F_2 = \sum_{a \in \mathbb{Z}^+(p)} t^{-a}(\phi * D_{a0}) + \alpha_0(\phi * D_0).$$

Therefore,

$$\sum_{a \in \mathbb{Z}^+(p)} t^{-a}(\phi * D_{a0}) + \alpha_0(\phi * D_0) \equiv \sum_{a \in \mathbb{Z}^+(p)} \phi^{-1}(t)^{-a} D_{a0} + \alpha_0 D_0 \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}}.$$

and the proposition is proved.

Consider $\mathrm{fr}_t \in \operatorname{Aut}\mathcal{K}$ such that $\mathrm{fr}_t(t) = t$ and $\mathrm{fr}_t|_k = \sigma$.

Proposition 2. *For all $a\in\mathbb{Z}^+(p)$ and $n\in\mathbb{Z}\operatorname{mod}N_0$, we have*

$$(\mathrm{fr}_t)*D_{an}=D_{a,n-1}.$$

Proof. Let $\hat\phi$ be a lifting of fr_t to $\operatorname{Aut}\mathcal{K}_{\mathrm{sep}}$. Set $F_1=\hat\phi^{-1}(F)$, then

$$\sigma F_1-F_1=\sum_{a\in\mathbb{Z}^+(p)}t^{-a}D_{a,-1}+(\sigma^{-1}\alpha_0)D_0.$$

Similarly to the previous proposition we obtain

$$\sum_{a\in\mathbb{Z}^+(p)}t^{-a}D_{a,-1}+(\sigma^{-1}\alpha_0)D_0\equiv\sum_{a\in\mathbb{Z}^+(p)}t^{-a}(\mathrm{fr}_t*D_{a0})+\alpha_0(\mathrm{fr}_t*D_0)\operatorname{mod}(\sigma-\mathrm{id})\mathcal{M}_{\mathcal{K}}.$$

This gives $\mathrm{fr}_t*D_{a0}=D_{a,-1}$ and the proposition follows from commutativity of fr_t and σ.

2. Preliminaries: ramification filtration modulo 3^{rd} commutators.

In this section $\mathcal{K}=k((t))$, where $k\simeq\mathbb{F}_{p^{N_0}}$ and t is a fixed uniformiser of $\mathcal{K}$. As earlier, $\mathcal{G}=\operatorname{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})$, and $\mathcal{G}(p)$ is the Galois group of the maximal p-extension of $\mathcal{K}$ in $\mathcal{K}_{\mathrm{sep}}$. We shall prove some auxiliary facts about structure of the ramification filtration $\{\mathcal{G}(p)^{(v)}\operatorname{mod}C_3(\mathcal{G}(p))\}_{1\leqslant v\leqslant v_0}$, where v_0 is some fixed rational number and $C_3(\mathcal{G}(p))$ is the closure of the subgroup of commutators of order $\geqslant 3$. This description comes as a special case of the general result from [Ab1,2]. We assume that $N_0\geqslant 2\log_p(pv_0)$.

2.1. Consider the profinite $\mathbb{Z}_p$-module $\hat{\mathcal{K}}^*$ from Section 1, and denote by $\widetilde{\mathcal{L}}$ the profree Lie algebra over $\mathbb{Z}_p$ with this module of generators. Denote by $\mathcal{L}$ the quotient of $\widetilde{\mathcal{L}}$ by the ideal of commutators of order $\geqslant p$, and consider the group $G(\mathcal{L})$ of its elements with composition law given by the Campbel-Hausdorff formula. Choose $\alpha_0\in W$ with trace 1 and use the uniformiser t of the field $\mathcal{K}$. The formalism of Artin-Schreier theory from n.1.2 can be generalised, cf. [Ab1], to construct the isomorphism

$$\psi:\mathcal{G}(p)/C_p(\mathcal{G}(p))\longrightarrow G(\mathcal{L})$$

(its construction depends on the above choice of $\alpha_0\in W$ and $t\in\mathcal{K}$). This isomorphism transfers the ramification filtration of the Galois group $\mathcal{G}$ to the filtration $\{\mathcal{L}^{(v)}\}_{v\geqslant -1}$ of the Lie algebra $\mathcal{L}$ by its "ramification ideals" $\mathcal{L}^{(v)}$, $v\geqslant -1$.

Consider corresponding extensions of scalars $\mathcal{L}_W=\mathcal{L}\otimes W$ and $\mathcal{L}_W^{(v)}=\mathcal{L}^{(v)}\otimes W$. For a given $v\geqslant 1$, explicit description of the ideal $\mathcal{L}_W^{(v)}$ can be given as follows.

Consider the W-basis $\mathcal{D}(t)=\{D_{an}\mid a\in\mathbb{Z}^+(p),n\in\mathbb{Z}\operatorname{mod}N_0\}\cup\{D_0\}$ of $\hat{\mathcal{K}}^*\otimes W$ from n.1.1. Set $D_{0n}=(\sigma^n\alpha_0)D_0$ for all $n\in\mathbb{Z}\operatorname{mod}N_0$. It will be convienient to use the notation $\mathbb{Z}^0(p)=\mathbb{Z}^+(p)\cup\{0\}$ and for all $a\in\mathbb{Z}^0(p)$ and $n\in\mathbb{Z}$, the notation D_{an} as well as the notation $D_{a,n\operatorname{mod}N_0}$. If $s\geqslant 1$ and $(n_1,\dots,n_s)\in\mathbb{Z}^s$, we set by definition

$$\eta(n_1,\dots,n_s)=\frac{1}{s_1!(s_2-s_1)!\dots(s_l-s_{l-1})!},$$

if for some $l \geqslant 1$ and $1 \leqslant s_1 < \dots < s_l = s$, one has $n_1 = \dots = n_{s_1} > \dots > n_{s_{l-1}} = \dots = n_{s_l}$, and we set

$$\eta(n_1, \dots, n_s) = 0,$$

otherwise.

If $\gamma \in \mathbb{Q}$, $\gamma > 0$ and $N \in \mathbb{N}$, set

$$\mathcal{F}_{\gamma,-N} = \sum (-1)^s \eta(n_1, \dots, n_s) a_1 p^{n_1} \left[\dots [D_{a_1 n_1}, D_{a_2 n_2}], \dots, \right],$$

where the sum is taken for all $1 \leqslant s < p$, $n_1 \geqslant 0$, $n_2, \dots, n_s \geqslant -N$ and $a_1, \dots, a_s \in \mathbb{Z}^0(p)$ such that $p^{n_1} a_1 + \dots + p^{n_s} a_s = \gamma$.

Then we define the ideal $\mathcal{L}_W^{(v)}(N)$ as the minimal σ-invariant ideal of $\mathcal{L}_W$ which contains all $\mathcal{F}_{\gamma,-N}$ with $\gamma \geqslant v$. Finally, in the above notation the description of the ramification filtration modulo commutators of order $\geqslant p$ is given by the following statement, cf. [Ab1,2]

Theorem. *There exists $N(v) \in \mathbb{N}$ such that the ideals $\mathcal{L}_W^{(v)}(N)$ do not depend on N if $N \geqslant N(v)$, and are equal to the ramification ideal $\mathcal{L}_W^{(v)}$.*

2.2. Consider the special case of the above general construction modulo the ideal $C_2(\mathcal{L}_W)$ of second commutators of the Lie algebra $\mathcal{L}_W$. Note that for any given $v \geqslant 1$, the ideals $\mathcal{L}_W^{(v)}(N) \bmod C_2(\mathcal{L}_W)$ coincide for all $N \geqslant 0$. So, the ideal $\mathcal{L}_W^{(v)} \bmod C_2(\mathcal{L}_W)$ appears as the W-submodule of $\hat{\mathcal{K}}^* \otimes W$ generated by the elements $p^s a D_{an}$, where $a \in \mathbb{Z}^+(p)$, $s \in \mathbb{Z}_{\geqslant 0}$ and $p^s a \geqslant v$. Clearly, this module comes from the subgroup of principal units of the valuation ring $O_{\mathcal{K}}$ of $\mathcal{K}$ congruent to 1 modulo t^v (what is very well-known from class field theory).

2.3. We need to simplify the general construction from n.2.1 to work with ramification filtration modulo commutators of order $\geqslant 3$.

First, we simplify the notation by setting $L = \mathcal{L} \bmod C_3(\mathcal{L})$, $L_W = \mathcal{L}_W \bmod C_3(\mathcal{L}_W)$, $L^{(v)} = \mathcal{L}^{(v)} \bmod C_3(\mathcal{L})$ and $L_W^{(v)} = \mathcal{L}_W^{(v)} \bmod C_3(\mathcal{L}_W)$ for all $v \geqslant 1$. Introduce new generators of the Lie algebra L_W related more closely to the ramification filtration. Note that the elements $\mathcal{F}_{\gamma,-N} \bmod C_3(\mathcal{L}_W)$ does not depend on $N \in \mathbb{Z}_{\geqslant 0}$ if $\gamma \in \mathbb{N}$. We use these elements to set

$$\Delta_{a0} = (1/a) \mathcal{F}_{a0} \bmod C_3(\mathcal{L}_W)$$

for all $a \in \mathbb{Z}^+(p)$. We set also $\Delta_{an} := \sigma^n \Delta_{a0}$ and note that

$$\Delta_{an} \bmod C_2(L_W) = D_{an} \bmod C_2(\mathcal{L}_W),$$

for all $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \bmod N_0$. So, if we define $\Delta_0 = D_0$, then we obtain the system of generators of the Lie W-algebra L_W

$$\{\Delta_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\} \cup \{\Delta_0\}.$$

Clearly, the description of the ramification filtration $L_W^{(v)} \bmod C_2(L_W)$ in new generators coincide with its description in terms of generators D_{an} from n.2.2.

In terms of new generators we have also:

— if $\gamma = ap^m$ with $a \in \mathbb{Z}^+(p)$ and $m \in \mathbb{Z}_{\geqslant 0}$, then

$$\mathcal{F}_{\gamma 0} \operatorname{mod} C_3(\mathcal{L}_W) = ap^m \Delta_{am} - \frac{1}{2} \sum p^s a_1 [\Delta_{a_1 s}, \Delta_{a_2 s}],$$

where the sum is taken for all $a_1, a_2 \in \mathbb{Z}^+(p)$ and $0 \leqslant s < m$ under the condition $p^s(a_1 + a_2) = \gamma$;

— if $\gamma \notin \mathbb{N}$, then

$$\mathcal{F}_{\gamma,-N} \operatorname{mod} C_3(\mathcal{L}_W) = -\sum p^{n_1} a_1 [\Delta_{a_1 n_1}, \Delta_{a_2 n_2}],$$

where the sum is taken for all $a_1, a_2 \in \mathbb{Z}^+(p)$ and $n_1 \geqslant 0$ and $n_2 \geqslant -N$ under the condition $p^{n_1} a_1 + p^{n_2} a_2 = \gamma$.

Take some $v \geqslant 1$. If $\gamma \geqslant v$ and $\gamma = ap^m \in \mathbb{N}$ with $a \in \mathbb{Z}^+(p)$ and $m \in \mathbb{Z}_{\geqslant 0}$, set

$$\mathcal{F}_\gamma^{(v)} = ap^m \Delta_{am} - \frac{1}{2} \sum p^s a_1 [\Delta_{a_1 s}, \Delta_{a_2 s}],$$

where the sum is taken for $a_1, a_2 \in \mathbb{Z}^+(p)$ and $0 \leqslant s < m$ such that $p^s a_1, p^s a_2 < v$ and $p^s(a_1 + a_2) = \gamma$.

If $\gamma \notin \mathbb{N}$ and $\gamma \geqslant v$, set

$$\mathcal{F}_\gamma^{(v)} = -\sum p^{n_1} a_1 [\Delta_{a_1 n_1}, \Delta_{a_2 n_2}],$$

where the sum is taken for $a_1, a_2 \in \mathbb{Z}^+(p)$ and $n_1 \geqslant 0$ such that $p^{n_1} a_1, p^{n_1} a_2 < v$ and $p^{n_1} a_1 + p^{n_2} a_2 = \gamma$.

Proposition. *In the above notation for any $v \geqslant 1$, $L_W^{(v)}$ is the minimal σ-invariant ideal of L_W containing the elements $\mathcal{F}_\gamma^{(v)}$ for all $\gamma \geqslant v$.*

Proof. Let $n^*(v)$ be the maximal integer $< \log_p(v/\{v\})$, where $\{v\}$ denotes the usual fractional part of v if $v \notin \mathbb{Z}$ and is equal to 1, if $v \in \mathbb{Z}$. Then we have the following property:

if $\gamma = p^{n_1} a_1 + p^{n_2} a_2 \geqslant v$ with $p^{n_1} a_1, p^{n_1} a_2 < v$, then $n_2 \geqslant n_1 - n^*(v)$.

Indeed, this follows from the inequality

$$p^{n_1 - n_2} = \frac{p^{n_1} a_2}{\gamma - p^{n_1} a_1} < \frac{v}{\{v\}}.$$

Therefore, for any $\gamma \geqslant v$ and $N \geqslant n^*(v)$, the above element $\mathcal{F}_\gamma^{(v)}$ differs from the element $\mathcal{F}_{\gamma,-N} \operatorname{mod} C_3(\mathcal{L}_W)$ by an element from the ideal $[L_W^{(v)}, L_W]$. The proposition is proved.

2.4. Denote by $L_{triv}^{(v)}$ the W-submodule of the W-module L_W containing the elements $p^s \Delta_{an}$ such that $p^s a \geqslant pv$, and the elements $p^s[\Delta_{a_1 n_1}, \Delta_{a_2 n_2}]$, such that $\max\{p^s a_1, p^s a_2\} \geqslant v$ (here $a, a_1, a_2 \in \mathbb{Z}^+(p)$, $n, n_1, n_2 \in \mathbb{Z} \operatorname{mod} N_0$ and $s \in \mathbb{Z}_{\geqslant 0}$). It is easy to see that $L_{triv}^{(v)}$ is generated by elements $\sigma^n \mathcal{F}_\gamma^{(v)}$ with $\gamma \geqslant pv$ and elements from $[L_W^{(v)}, L_W]$. Therefore, $L_{triv}^{(v)} \subset L_W^{(v)}$.

Let

$$S_1 = \{(a,n) \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\},$$

$$S_2 = \{(a_1,n_1,a_2,n_2) \mid a_1,a_2 \in \mathbb{Z}^+(p), n_1,n_2 \in \mathbb{Z} \bmod N_0\}.$$

If $(a,n) \in S_1$, set $s = s(a)$ for the integer s such that $v \leqslant p^s a < pv$, and set

$$\gamma(a,n) = p^{s(a)}a.$$

Denote by $S^{(v)}_{1,adm}$ the subset of elements $(a,n) \in S_1$ such that $s(a) \in \mathbb{Z}_{\geqslant 0}$.

If $(a_1,n_1,a_2,n_2) \in S_2$, set $s = s(a_1,a_2)$ for the maximal integer s such that $\max\{p^s a_1, p^s a_2\} < v$. If $n^*_{12} \in \mathbb{Z}$ is such that $n^*_{12} \bmod N_0 = n_1 - n_2$ and $0 \leqslant n^*_{12} < N_0$, we set

$$\gamma(a_1,n_1,a_2,n_2) = p^{s(a_1,a_2)}\left(a_1 + \frac{a_2}{p^{n^*_{12}}}\right).$$

Denote by $S^{(v)}_{2,adm}$ the subset of $(a_1,n_1,a_2,n_2) \in S_2$ such that $s(a_1,a_2) \in \mathbb{Z}_{\geqslant 0}$, $\gamma(a_1,n_1,a_2,n_2) \geqslant v$, and if $n_1 = n_2$ then $a_1 > a_2$ and $a_1 + a_2 \equiv 0 \bmod p$.

Denote by $L^{(v)}_{adm}$ the submodule of L_W generated by elements from $L^{(v)}_{triv}$ and by elements $p^{s(a)}\Delta_{an}$ and $p^{s(a_1,a_2)}[\Delta_{a_1n_1}, \Delta_{a_2n_2}]$, where $(a,n) \in S^{(v)}_{1,adm}$ and $(a_1,n_1,a_2,n_2) \in S^{(v)}_{2,adm}$.

Proposition 1. $L^{(v)}_{adm} \supset L^{(v)}_W \supset L^{(v)}_{triv} \supset pL^{(v)}_{adm}$.

Proof. The inclusion $pL^{(v)}_{adm} \subset L^{(v)}_{triv}$ follows directly from definitions. The inclusion $L^{(v)}_{triv} \subset L^{(v)}_W$ was explained in the beginning of this subsection.

In order to prove that $L^{(v)}_W \subset \mathcal{L}^{(v)}_{adm}$, it is sufficient to verify that for any $\gamma \geqslant v$, we have $\mathcal{F}^{(v)}_\gamma \in L^{(v)}_{adm}$.

This follows directly from the definition of $S^{(v)}_{2,adm}$ in the case $\gamma \notin \mathbb{N}$.

If $\gamma = ap^m \in \mathbb{N}$ with $a \in \mathbb{Z}^+(p)$ and $m \in \mathbb{Z}_{\geqslant 0}$, we note that

$$\mathcal{F}^{(v)}_\gamma \equiv ap^m\Delta_{am} - \sum p^s a_1[\Delta_{a_1s}, \Delta_{a_2s}] \bmod L^{(v)}_{triv},$$

where the sum is taken for all $a_1,a_2 \in \mathbb{Z}^+(p)$ and $0 \leqslant s < m$, such that $a_1 > a_2$ and $p^s(a_1+a_2) = ap^m$ (one has $a_1 + a_2 \equiv 0 \bmod p$ because $s < m$). The proposition is proved.

Proposition 2. *Let $1 \leqslant v \leqslant v_0$ and $pv \in \mathbb{N}$. Then images of elements from the sets*

$$\{p^{s(a)}\Delta_{an} \mid (a,n) \in S^{(v)}_{1,adm}\}$$

and

$$\{p^{s(a_1,a_2)}[\Delta_{a_1n_1}, \Delta_{a_2n_2}] \mid (a_1,n_1,a_2,n_2) \in S^{(v)}_{2,adm}\}$$

in the k-module $L^{(v)}_{adm}/L^{(v)}_{triv}$ are linearly independent (and therefore, give its k-basis).

Proof. It is sufficient to verify the following implication

$$(a_1,n_1,a_2,n_2) \in S^{(v)}_{2,adm} \quad \Rightarrow \quad (a_2,n_2,a_1,n_1) \notin S^{(v)}_{2,adm}.$$

Indeed, if $n_1 = n_2$, then $a_1 > a_2$ by definition, and therefore, in this case $(a_2, n_2, a_1, n_1) \notin S^{(v)}_{2,adm}$.

Assume that $n_1 \neq n_2$. If $s = s(a_1, a_2)$, then

$$p^s \left(a_1 + \frac{a_2}{p^{n^*_{12}}} \right) \geqslant v,$$

because $(a_1, n_1, a_2, n_2) \in S^{(v)}_{2,adm}$. Because $pv \in \mathbb{N}$ and $p^s a_1 < v \leqslant v_0$, we have $v - p^s a_1 \geqslant 1/p$, and therefore, $p^{n^*_{12}} \leqslant p^s a_2 (1/p)^{-1} < pv_0$, i.e. $n^*_{12} < \log_p(pv_0)$.

Similarly, if we assume that $(a_2, n_2, a_1, n_1) \in S_{2,adm}$, then $n^*_{21} < \log_p(pv_0)$. But this gives the contradiction

$$2 \log_p(pv_0) \leqslant N_0 = n^*_{12} + n^*_{21} < 2 \log_p(pv_0).$$

The proposition is proved.

Consider an arbitrary element $l \in L^{(v)}_{adm} \bmod L^{(v)}_{triv}$. Then it can be presented in the following form

$$\sum_{(a,n) \in S^{(v)}_{1,adm}} \alpha_{an} p^{s(a)} \Delta_{an} + \sum_{(a_1,n_1,a_2,n_2) \in S^{(v)}_{2,adm}} \alpha_{a_1 n_1 a_2 n_2} p^{s(a_1,a_2)} [\Delta_{a_1 n_1}, \Delta_{a_2 n_2}]$$

with some coefficients α_{an} and $\alpha_{a_1 n_1 a_2 n_2}$ from the residue field k.

Introduce the following subset of rational numbers

$$\Gamma_{adm}(v) = \{\gamma(a, n) \mid (a, n) \in S^{(v)}_{1,adm}\} \cup \{\gamma(a_1, n_1, a_2, n_2) \mid (a_1, n_1, a_2, n_2) \in S^{(v)}_{2,adm}\}.$$

Clearly, the elements from the set

$$S(v) = \{\sigma^n \mathcal{F}^{(v)}_\gamma \mid \gamma \in \Gamma_{adm}(v), n \in \mathbb{Z} \bmod N_0\}$$

generate the k-module $L^{(v)}_W$. But expressions of any two different elements of this set in terms of the k-basis from above Proposition 2 do not have common terms (with non-zero coefficients). Therefore, elements of the set $S(v)$ give a k-basis of $L^{(v)}_W$ modulo $L^{(v)}_{triv}$. We state this property as the following proposition.

Proposition 3. *In the above notation the element $l \in L^{(v)}_{adm} \bmod L^{(v)}_{triv}$ comes from the ramification ideal $L^{(v)}_W$ if and only if for all $\gamma \in \Gamma_{adm}(v)$ and $m \in \mathbb{Z} \bmod N_0$, there exist $A_{\gamma,m} \in k$, such that*

1) *if $(a, n) \in S^{(v)}_{1,adm}$, $\gamma = \gamma(a, n)$ and $n = s(a) + m$, then $a^{-1} \alpha_{an} = A_{\gamma,m}$;*

2) *if $(a_1, n_1, a_2, n_2) \in S^{(v)}_{2,adm}$, $\gamma = \gamma(a_1, n_1, a_2, n_2)$ and $n_1 = s(a_1, a_2) + m$, then $a_1^{-1} \alpha_{a_1,n_1,a_2,n_2} = -A_{\gamma,m}$.*

3. The main lemma.

In this section $\mathcal{K}$ is a complete discrete valuation field of characteristic p with finite residue field $k \simeq \mathbb{F}_{p^{N_0}}$, $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})$ and $\{\mathcal{G}^{(v)}\}_{v \geqslant -1}$ — the ramification filtration of $\mathcal{G}$ in upper numbering. We also use all notation introduced in Sections 1 and 2.

3.1. Assume that $p \geqslant 5$ and v_0 is a natural number such that $v_0 \equiv 0 \bmod p^2$. We assume that $N_0 \geqslant 2\log_p(p^2 v_0)$. We note that N_0 certainly satisfies the assumption $N_0 \geqslant 2\log_p(pv_0)$ from Section 2.

Consider the quotient

$$\bar{\mathcal{G}} = \mathcal{G}/\mathcal{G}^{p^3} C_3(\mathcal{G})$$

with filtration $\{\bar{\mathcal{G}}^{(v)}\}_{v \geqslant -1}$ induced by the ramification filtration of the group $\mathcal{G}$. As in Section 1 we set $\mathcal{M} = \mathcal{G}/\mathcal{G}^p C_2(\mathcal{G})$. Then the ramification filtration of $\mathcal{M}$ coincides, in fact, with its filtration by submodules $\mathcal{M}^{(a)}$, $a \in \mathbb{N}$, cf. n.1.5.

Assume $\bar{F} : \bar{\mathcal{G}} \longrightarrow \bar{\mathcal{G}}$ is a group automorphism such that for any rational number v such that $1 \leqslant v \leqslant v_0$, we have $\bar{F}(\bar{\mathcal{G}}^{(v)}) = \bar{\mathcal{G}}^{(v)}$. We note, the existence of such morphism $\bar{F}$ is equivalent to the existence of a compatible with ramification filtration group automorphism of the quotient $\bar{\mathcal{G}}/\bar{\mathcal{G}}^{(v_0)}$.

Consider extension of scalars $f_k : \mathcal{M}_k \longrightarrow \mathcal{M}_k$ of the morphism $f : \mathcal{M} \longrightarrow \mathcal{M}$ induced by $\bar{F}$. Clearly, for any $1 \leqslant a \leqslant v_0$, we have $f_k(\mathcal{M}_k^{(a)}) = \mathcal{M}_k^{(a)}$. Take uniformising element $t \in \mathcal{K}$ and consider corresponding special basis of $\mathcal{M}_k^{(1)}$

$$\mathcal{D}^{(1)}(t) \bmod p = \{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\}.$$

Set

$$f_k(D_{a0}) = \sum_{\substack{b \in \mathbb{Z}^+(p) \\ m \in \mathbb{Z} \bmod N_0}} \alpha_{abm} D_{bm},$$

where all $\alpha_{abm} \in k$. Clearly, $\alpha_{abm} = 0$ if $b < a < v_0$.

If $m \in \mathbb{Z} \bmod N_0$ we use the notation $\hat{m}$ for the unique natural number satisfying the conditions $0 \leqslant \hat{m} < N_0$ and $\hat{m} \bmod N_0 = m$.

With the above notation and assumptions we have the following statement.

Main Lemma. *Assume that:*
— $\alpha_{110} = 1$*;*
— $\alpha_{1b0} = 0$ *for all* $b \in \mathbb{Z}^+(p), 1 < b < v_0$*;*
— $\alpha_{2b0} = 0$ *for all* $b \equiv 1 \bmod p, 1 < b < v_0$.
Then for all $1 \leqslant a < b < v_0/p$ *such that* $a, b \in \mathbb{Z}^+(p)$ *and* $m \not\equiv 0 \bmod N_0$*, we have:*
a) $\alpha_{aa0} = 1$ *and* $\alpha_{ab0} = 0$*;*
b) *if* $b/p^{\hat{m}} < a$*, then* $\alpha_{a,b,-m} = 0$*;*
c) *there exist elements* $\beta_{c,m} \in k$*, where* $c \in \mathbb{Z}^+(p)$*, such that if* $c = b - ap^{\hat{m}}$ *then* $\alpha_{a,b,-m} = \beta_{c,-m}$.

Remark. Finally, the morphism f_k is given by the correspondences

$$D_{a0} \mapsto D_{a0} + \sum_{\substack{m \not\equiv 0 \bmod N_0 \\ c \in \mathbb{Z}^+(p)}} \beta_{c,-m} D_{ap^{\hat{m}}+c,-m} \bmod \mathcal{M}_k^{(v_0/p)},$$

where $a \in \mathbb{Z}^+(p)$ and $1 \leqslant a < v_0/p$. It can be also shown that any such morphism comes from some automorphism of the group $\mathcal{G}(p)/C_3(\mathcal{G}(p))$ respecting ramification filtration for all rational upper numbers v such that $1 \leqslant v \leqslant v_0/p$.

Proof of main lemma.

3.2. Choose $\alpha_0 \in W$ with trace 1, and use the uniformizer t to construct the identification $\psi : \mathcal{G}(p)/C_p(\mathcal{G}(p)) \simeq G(\mathcal{L})$ from n.2.1. Then in the notation of n.2, the group $\bar{\mathcal{G}}$ is identified with $G(\bar{L})$, where $\bar{L} = L/p^3L$ is a Lie algebra over $\mathbb{Z}_p$, and the ramification filtration of the group $\bar{\mathcal{G}}$ corresponds to the filtration of $\bar{L}$ by its ideals $\bar{L}^{(v)} = L^{(v)} \operatorname{mod} p^3L$, $v \geqslant 1$. Under this identification, the group automorphism $\bar{F}$ gives rise to the automorphism $\bar{F}$ of the Lie algebra $\bar{L}$. Consider extensions of scalars $\bar{L}_W = \bar{L} \otimes W = L_W \operatorname{mod} p^3 L_W$ and $\bar{L}_W^{(v)} = \bar{L}^{(v)} \otimes W = L_W^{(v)} \operatorname{mod} p^3 L_W$, where $v \geqslant 1$.

Without special mentioning we shall put a bar to any notation related to the Lie algebra $\bar{L}$ if it came from the similar notation introduced earlier for the algebra L.

The automorphism $\bar{F}_W$ of the Lie algebra $\bar{L}_W$ commutes with Frobenius and satisfies the condition

$$\bar{F}_W(\bar{L}_W^{(v)}) = \bar{L}_W^{(v)}$$

for all $1 \leqslant v \leqslant v_0$. We can use the description of the filtration $\{L_W^{(v)}\}_{v \geqslant 1}$ from n.2 to obtain the description of the induced filtration $\{\bar{L}_W^{(v)}\}_{v \geqslant 1}$ in terms of generators $\bar{\Delta}_{an} = \Delta_{an} \operatorname{mod} p^3$ (where $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \operatorname{mod} N_0$) and $\bar{\Delta}_0 = \Delta_0 \operatorname{mod} p^3$. Note that for any $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \operatorname{mod} N_0$,

$$\bar{F}_W(\bar{\Delta}_{an}) \equiv \sum_{\substack{b \in \mathbb{Z}^+(p) \\ m \in \mathbb{Z} \operatorname{mod} N_0}} \sigma^n(\alpha_{abm}) \bar{\Delta}_{b,m+n} \operatorname{mod} \left(C_2(\bar{L}_W) + p\bar{L}_W \right).$$

Proposition 1. *If $n \not\equiv 0 \operatorname{mod} N_0$, then $\alpha_{11n} = 0$.*

Proof. Let $v = 2 + 1/p$. Then $(1/2)\bar{\mathcal{F}}_v^{(v)} = [\bar{\Delta}_{2,0}, \bar{\Delta}_{1,-1}] \in \bar{L}_W^{(v)}$ is mapped by $\bar{F}_W$ to

$$\sum_{n,m \in \mathbb{Z} \operatorname{mod} N_0} \alpha_{22m} \sigma^{-1}(\alpha_{11n}) [\bar{\Delta}_{2,-m}, \bar{\Delta}_{1,-n-1}] +$$

$$\sum_{n,m \in \mathbb{Z} \operatorname{mod} N_0} \alpha_{22m} \sigma^{-1}(\alpha_{12n}) [\bar{\Delta}_{2,-m}, \bar{\Delta}_{2,-n-1}] \operatorname{mod} \left(\bar{L}_{triv}^{(v)} + p\bar{L}_W \right).$$

It is easy to see that $\bar{L}_{adm}^{(v)} \operatorname{mod} \bar{L}_{triv}^{(v)}$ has the following k-basis

$$\{\sigma^n \Delta_{10}, \sigma^n \Delta_{20}, \sigma^n [\Delta_{20}, \Delta_{1,-1}], \sigma^n [\Delta_{20}, \Delta_{2,-1}] \mid n \in \mathbb{Z} \operatorname{mod} N_0\}.$$

From $\alpha_{110} \neq 0$, we obtain $\alpha_{22m} = 0$ for all $m \neq 0$, but this implies $\alpha_{220} \neq 0$ and, therefore, $\alpha_{11n} = 0$, if $n \not\equiv 0 \operatorname{mod} N_0$. The proposition is proved.

Proposition 2. *If $a \in \mathbb{Z}^+(p)$, $1 < a < v_0$ and $n \not\equiv 0 \operatorname{mod} N_0$, then $\alpha_{aan} = 0$.*

Proof. Assume that for some $n \not\equiv 0 \operatorname{mod} N_0$, we have $\alpha_{aan} \neq 0$.

Take $v = a + 1/p$, and consider

$$\bar{\mathcal{F}}_v^{(v)} = \sum a_1 [\bar{\Delta}_{a_1 0}, \bar{\Delta}_{a_2,-1}] = a[\bar{\Delta}_{a0}, \bar{\Delta}_{1,-1}] + \cdots \in \bar{L}_W^{(v)} \operatorname{mod} p\bar{L}_W,$$

where the sum is taken for all $a_1, a_2 \in \mathbb{Z}^+(p)$ such that $a_1 + a_2/p = v$ and $a_1, a_2 \leqslant a$. The expression for $\bar{F}_W(\bar{\mathcal{F}}_v^{(v)})$ contains the commutator $[\bar{\Delta}_{an}, \bar{\Delta}_{1,-1}]$ with non-zero coefficient $a\alpha_{aan}$. This commutator belongs to $\bar{L}_{adm}^{(v)} \bmod p$ only if $\gamma(a,n,1,-1) \geqslant v$.

Because $n \not\equiv 0 \bmod N_0$, this implies that $n = -1 \bmod N_0$ and $a + 1 \equiv 0 \bmod p$. The commutator $[\bar{\Delta}_{a,-1}, \bar{\Delta}_{1,-1}]$ appears in the expression of $\sigma^{-1}\bar{\mathcal{F}}_{a+1}^{(v)}$ with non-zero coefficient, therefore,

$$\bar{F}_W(\bar{\mathcal{F}}_v^{(v)}) \bmod \bar{L}_{triv}^{(v)} + p\bar{L}_W$$

must contain another term $[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{2,-1}]$ of $\sigma^{-1}\bar{\mathcal{F}}_{a+1}^{(v)}$ also with non-zero coefficient (we use that $p \geqslant 5$ and therefore, $a \geqslant 4$).

This is impossible, because

$$\bar{F}_W(\bar{\mathcal{F}}_v^{(v)}) \bmod \bar{L}_{triv}^{(v)} + p\bar{L}_W$$

is a linear combination of commutators of the form $[\bar{\Delta}_{b_1 n_1}, \bar{\Delta}_{b_2 n_2}]$, where $b_1 \geqslant a_1$, $b_2 \geqslant a_2$, and $a_1 + (a_2/p) = v$, with $1 \leqslant a_1, a_2 \leqslant a$ (indeed, if $b_1 = a - 1$, then $2 = b_2 \geqslant p + 1$ gives contradiction; if $b_1 = 2$, then $a_1 \leqslant 2$, but then $a \geqslant a_2 \geqslant p(a-2) + 1/p$ gives contradiction). The proposition is proved.

3.3. For $a \in \mathbb{Z}^+(p)$, $a < v_0$, set for simplicity $\alpha_{aa0} = \alpha_a$.

Proposition. *There exists $\lambda \in k$ such that for all $a \in \mathbb{Z}^+(p)$, one has $\alpha_a = \lambda^{a-1}$.*

Proof.

Lemma 1. *If $a > p$, $a \not\equiv 1 \bmod p$, then $\alpha_a = \alpha_{a-1}\sigma^{-1}(\alpha_{p+1})$.*

Proof. Take $v = a + 1/p$. Then

$$\bar{\mathcal{F}}_v^{(v)} = a[\bar{\Delta}_{a0}, \bar{\Delta}_{1,-1}] + (a-1)[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{p+1,-1}] + \dots$$

The image of $\bar{\mathcal{F}}_v^{(v)}$ modulo $\bar{L}_{triv}^{(v)} + p\bar{L}_W$ contains the term $a[\bar{\Delta}_{a0}, \bar{\Delta}_{1,-1}]$ with coefficient α_a, and the term $(a-1)[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{p+1,-1}]$ with coefficient $\alpha_{a-1}\sigma^{-1}(\alpha_{p+1})$. So, the lemma follows from Proposition 3 of n.2.4.

We note, the above lemma implies that $\alpha_a = \lambda^{a-1}$ for $p < a < 2p$ with $\lambda := \sigma^{-1}(\alpha_{p+1})$.

Lemma 2. $\alpha_a = \lambda^{a-1}$ *for* $1 \leqslant a < p$.

Proof. Take $v = 2p - 1 + a/p$ for $1 \leqslant a < p$. The image of $\bar{\mathcal{F}}_v^{(v)}$ modulo $\bar{L}_{triv}^{(v)} + p\bar{L}_W$ contains the term $(2p-1)[\bar{\Delta}_{2p-1,0}, \bar{\Delta}_{a,-1}]$ with coefficient $\alpha_{2p-1}\sigma^{-1}(\alpha_a)$, and the term $(2p-2)[\bar{\Delta}_{2p-2,0}, \bar{\Delta}_{p+a,-1}]$ with coefficient $\alpha_{2p-2}\sigma^{-1}(\alpha_{p+a})$. This gives by Proposition 3 of n.2.4, that $\alpha_{2p-1}\sigma^{-1}(\alpha_a) = \alpha_{2p-2}\sigma^{-1}(\alpha_{p+a})$, and therefore, $\alpha_a = \sigma(\lambda)^{-1}\alpha_{a+p} = \lambda^{a-1}$. The lemma is proved.

Lemma 3. $\alpha_{2p+1} = \lambda^{2p}$.

Proof. Take $v = 2p + 3 + 1/p$. The image of $\bar{\mathcal{F}}_v^{(v)}$ contains the term

$$(2p+3)[\bar{\Delta}_{2p+3,0}, \bar{\Delta}_{1,-1}]$$

with coefficient α_{2p+3}, and the term

$$(2p+1)[\bar{\Delta}_{2p+1,0}, \bar{\Delta}_{2p+1,-1}]$$

with coefficient $\alpha_{2p+1}\sigma^{-1}(\alpha_{2p+1})$. So, $\alpha_{2p+3}=\alpha_{2p+1}\sigma^{-1}(\alpha_{2p+1})$ by the proposition 3 of n.2.4. From the above lemma 1 we obtain $\alpha_{2p+3}=\lambda^2\alpha_{2p+1}$, and therefore, $\alpha_{2p+1}=\lambda^{2p}$.

We finish the proof of proposition by induction on a. It has been proved already, that $\alpha_a=\lambda^{a-1}$ for $a\leqslant 2p-1$.

Assume that $a\in\mathbb{Z}^+(p)$, $v_0>a>2p+1$ and for any $b\in\mathbb{Z}^+(p)$, $b<a$, we have $\alpha_b=\lambda^{b-1}$.

If $a\not\equiv 1 \bmod p$, then $\alpha_a=\lambda^{a-1}$ by lemma 1. If $a\equiv 1\bmod p$, then $a\geqslant 3p+1$. Take $v=a+1/p$. Then the image of $\bar{\mathcal{F}}_v^{(v)}$ contains the term $a[\bar\Delta_{a0},\bar\Delta_{1,-1}]$ with coefficient α_a, and the term $(a-2)[\bar\Delta_{a-2,0},\bar\Delta_{2p+1,-1}]$ with coefficient $\alpha_{a-2}\sigma^{-1}\alpha_{2p+1}$. Therefore, $\alpha_a=\alpha_{a-2}\sigma^{-1}\alpha_{2p+1}=\lambda^{a-1}$.

The proposition is proved.

3.4. Consider $\lambda\in k$ from above n.3.3.

Proposition. $\lambda=1$.

Proof. Consider the image $\bar F_W(\bar{\mathcal{F}}_{p^2}^{(p^2)}) \bmod \bar L_{triv}^{(p^2)}$ of

$$\bar{\mathcal{F}}_{p^2}^{(p^2)}=p^2\bar\Delta_{1,2}-\sum_{\substack{a_1+a_2=p\\ a_1>a_2\\ a_1,a_2\in\mathbb{Z}^+(p)}} pa_1[\bar\Delta_{a_1,1},\bar\Delta_{a_2,1}]-\sum_{\substack{a_1+a_2=p^2\\ a_1>a_2\\ a_1,a_2\in\mathbb{Z}^+(p)}} a_1[\bar\Delta_{a_1,0},\bar\Delta_{a_2,0}]\in\bar L_W^{(p^2)}.$$

Following the terms of $\bar{\mathcal{F}}_{p^2}^{(p^2)}$ in this image, we obtain by Proposition 3 of n.2.4 the equalities $1=\lambda^{p(p-2)}=\lambda^{p^2-2}$, and they imply that $\lambda=1$.

3.5. We need the following lemma in the nn.3.6-3.7 below.

Lemma. *If $a,b\in\mathbb{Z}^+(p)$, $a<b<v_0$ and $b/p<a$, then $\alpha_{a,b,-1}=0$.*

Proof. Assume that $\alpha_{a,b,-1}\neq 0$. Take $v=b+a/p^m$, where m is the minimal integer such that $p^m\geqslant v_0$. Then $b<v<b+1\leqslant v_0$ and, therefore,

$$\bar{\mathcal{F}}_v^{(v)}\equiv b[\bar\Delta_{b0},\bar\Delta_{a,-m}] \bmod \bar L_{triv}^{(v)}+p\bar L_W.$$

By Proposition of n.3.4, the image

$$\bar F_W(\bar{\mathcal{F}}_v^{(v)}) \bmod \bar L_{triv}^{(v)}+p\bar L_W$$

contains the term $[\bar\Delta_{b0},\bar\Delta_{b,-(m+1)}]$ with non-zero coefficient $\sigma^{-m}(\alpha_{a,b,-1})$. Therefore,

$$\max\{\gamma(b,0,b,-(m+1)),\gamma(b,-(m+1),b,0)\}\geqslant v,$$

cf. notation n.2.5. Clearly, $1\leqslant m+1<\log_p(v_0)+2<N_0$, therefore,

$$\gamma(b,0,b,-(m+1))=b\left(1+\frac{1}{p^{m+1}}\right),\quad \gamma(b,-(m+1),b,0)=b\left(1+\frac{1}{p^{N_0-(m+1)}}\right).$$

Because $\gamma(b,0,b,-(m+1))<b+a/p^m=v$, it is sufficient to verify that $\gamma(b,-(m+1),b,0)\leqslant\gamma(b,0,b,-(m+1))$ or, equivalently, $N_0\geqslant 2(m+1)$. Indeed,

$$2(m+1)<2(\log_p(v_0)+2)=2\log_p(p^2v_0)\leqslant N_0.$$

The lemma is proved.

3.6. For any $a,b\in\mathbb{Z}^+(p)$ such that $1\leqslant a<b<v_0$, we shall use the simpler notation $\alpha_{ab}=\alpha_{ab0}$.

Proposition. *Assume that for some $r \in \mathbb{Z}_{\geqslant 0}$ and all $l, l_1 \in \mathbb{Z}^+(p)$ such that*

$$l < l_1 \leqslant \min\{l + r, v_0 - 1\},$$

we have $\alpha_{ll_1} = 0$. Then for all $b, b_1 \in \mathbb{Z}^+(p)$ such that

$$p < b < b_1 < \min\{(r+1)p, v_0\},$$

we have $\alpha_{bb_1} = \alpha_{b-p, b_1-p}$.

Proof. Let $a = v_0 - 1$ and $v = a - 1 + b/p$. Then

$$\bar{\mathcal{F}}_v^{(v_0)} = \sum_{\substack{a'+b'/p=v \\ a', b' < v_0}} a'[\bar{\Delta}_{a'0}, \bar{\Delta}_{b',-1}] = a[\bar{\Delta}_{a0}, \bar{\Delta}_{b-p,-1}] + (a-1)[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{b,-1}] + \dots$$

Note that for any (a', b'), such that $a' + b'/p = v$, we have

$$pa' = p(v_0 - 1) + (b - p) - b' > (p-1)(v_0 - 1) \geqslant v_0.$$

Therefore, by Lemma of n.3.5, it holds $\alpha_{a',b_1,-1} = 0$. So, the image of $\bar{\mathcal{F}}_v^{(v_0)} \operatorname{mod} \bar{L}_{triv}^{(v_0)} + p\bar{L}_W$ contains the term $[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{b_1,-1}]$ with coefficient

$$\sum_{\substack{a', b' < v_0 \\ a'+b'/p=v}} a'\alpha_{a',a-1}\sigma^{-1}(\alpha_{b'b_1}).$$

But, if $a' \neq a-1$ and $\alpha_{a',a-1} \neq 0$, then $a' \leqslant (a-1) - (r+1)$, i.e. $a - 1 - a' \geqslant r + 1$. Because $a' + b'/p = a - 1 + b/p$, we have

$$b' \geqslant b + p(a - 1 - a') \geqslant b + p(r+1) > b_1,$$

and therefore, $\alpha_{b'b_1} = 0$. This proves that the coefficient for the term $[\bar{\Delta}_{a-1,0}, \bar{\Delta}_{b_1,-1}]$ equals $(a-1)\sigma^{-1}(\alpha_{bb_1})$.

Similarly, we obtain that the coefficient for the term $[\Delta_{a0}, \Delta_{b_1-p,-1}]$ is equal to $a\sigma^{-1}(\alpha_{b-p,b_1-p})$, and our proposition follows from Proposition 3 of n.2.4.

3.7. The following proposition proves the part a) of the Main Lemma.

Proposition. *Let $r \in \mathbb{Z}_{\geqslant 0}$ be such that $(r+2)p \leqslant v_0$. Then for any $l, l_1 \in \mathbb{Z}^+(p)$ such that $l < l_1 \leqslant \min\{l + r, v_0\}$, we have $\alpha_{ll_1} = 0$.*

Proof. We apply induction on r. So, we can assume that $\alpha_{ll_1} = 0$ for $l < l_1 < l + r$. By Proposition of n.3.6, this gives that $\alpha_{bb_1} = \alpha_{b-p,b_1-p}$ for $b < b_1 < b + rp$ (all indices are assumed to belong to the segment $[1, v_0)$).

In particular, we have $\alpha_{sp+1,b} = \alpha_{1,b-sp} = 0$ for $b < 1 + (s+r)p$ and $s \in \mathbb{N}$. .

We shall use the agreement $\bar{\Delta}_{a0} = 0$ and $\alpha_{ab} = 0$, if one of indices a or b is not prime to p. We introduce also the new notation $\alpha_m(n) := \alpha_{m,m+n}$, where $m, n \in \mathbb{N}$.

For $j = 1, \dots, p-1$, set $c_j = p(r+1) + j$ and $v_j = c_j + 1/p$, and consider

$$\bar{\mathcal{F}}_{v_j}^{(v_j)} \equiv c_j[\Delta_{c_j,0}, \Delta_{1,-1}] + \dots + (c_j - r - 1)[\Delta_{c_j-r-1,0}, \Delta_{p(r+1)+1,-1}] \operatorname{mod} p\bar{L}_W.$$

Note that $\alpha_{c,c',-1} = 0$, where $c \geqslant c_j - r - 1$ and $c' < v_j$. Indeed, this follows from Lemma of n.3.5, because

$$pc \geqslant p(c_j - r - 1) \geqslant p(p(r+1) - r) \geqslant p(r+2) > v_j > c'.$$

Therefore, all terms of the kind $[\bar{\Delta}_{*,0}, \bar{\Delta}_{*,-1}]$ appearing in the image of $\bar{\mathcal{F}}_{v_j}^{(v_j)}$ modulo $\bar{L}_{triv}^{(v_j)} + p\bar{L}_W$, can be written in the following way

$$c_j \left[\bar{\Delta}_{c_j,0}, \bar{\Delta}_{1,-1}\right] +$$

$$(c_j - 1)\left[\bar{\Delta}_{c_j-1,0}, \bar{\Delta}_{p+1,-1} + \alpha_{p+1}(rp)\bar{\Delta}_{(r+1)p+1,-1} + \dots\right] +$$

$$(c_j - 2)\left[\bar{\Delta}_{c_j-2,0}, \bar{\Delta}_{2p+1,-1}\right] + \dots +$$

$$(c_j - r)\left[\bar{\Delta}_{c_j-r,0} + \alpha_{c_j-r}(r)\bar{\Delta}_{c_j,0}, \bar{\Delta}_{rp+1,-1}\right] +$$

$$(c_j - r - 1)\left[\bar{\Delta}_{c_j-r-1,0} + \alpha_{c_j-r-1}(r)\bar{\Delta}_{c_j-1,0} + \alpha_{c_j-r}(r)\bar{\Delta}_{c_j,0}, \bar{\Delta}_{(r+1)p+1,-1}\right].$$

Consider the terms coming from $\bar{\mathcal{F}}_{\gamma}^{(v_j)}$, where

$$\gamma = c_j + \frac{rp+1}{p} = c_j - 1 + \frac{(r+1)p+1}{p}.$$

These terms are

$$(c_j - r)\alpha_{c_j-r}(r)\left[\bar{\Delta}_{c_j,0}, \bar{\Delta}_{rp+1,-1}\right] +$$

$$(c_j - 1)\sigma^{-1}(\alpha_{p+1}(rp))\left[\bar{\Delta}_{c_j-1,0}, \bar{\Delta}_{(r+1)p+1,-1}\right] +$$

$$(c_j - r - 1)\alpha_{c_j-r-1}(r)\left[\bar{\Delta}_{c_j-1,0}, \bar{\Delta}_{(r+1)p+1,-1}\right].$$

Therefore, for $j = 2, \dots, p-1$, we obtain the equalities

$$\frac{(j-r)\alpha_{c_j-r}(r)}{j} = \frac{(j-r-1)\alpha_{c_j-r-1}(r)}{j-1} + \sigma^{-1}(\alpha_{p+1}(rp))$$

(we use that $c_j \equiv j \bmod p$).

Set $X = \sigma^{-1}\alpha_{p+1}(rp)$ and $\beta_j = (j-r)\alpha_{c_j-r}(r)/j$ for $j = 1, \dots, p-1$. Then the above equalities can be rewritten in the form

$$\beta_2 = \beta_1 + X, \quad \dots \quad, \beta_{p-1} = \beta_{p-2} + X.$$

But now we use that:

a) $\beta_r = 0$, if $r \not\equiv 0 \bmod p$;

b) if $r \not\equiv -1 \bmod p$, then $\beta_{r+1} = 0$ (this follows from the property $\alpha_1(r) = 0$, cf. the statement of main lemma), and if $r \equiv -1 \bmod p$, then $\beta_1 = 0$ (this follows from the property $\alpha_2(r) = 0$, cf. loc.cit).

In the case $r \not\equiv 0 \bmod p$, this gives $X = \beta_1 = \dots = \beta_{p-1} = 0$. Therefore, for all $(r+1)p < a < (r+2)p$, we have $\alpha_{a-r,a} = 0$. So, in this case our proposition follows from Proposition of n.3.6.

Consider the case $r\equiv 0 \bmod p$. Here we have only that $\alpha_{c_j-r}(r)=(j-1)X$ for all $1\leqslant j<p$. By Proposition of n.3.6 this gives

$$\alpha_a(r)=(a-1)X$$

for all $a\in\mathbb{Z}^+(p)$ such that $a<(r+2)p-r$.

Consider the natural number b such that $b=r/p+1$, if $r\not\equiv -p \bmod p^2$, and $b=r/p+2$, if $r\equiv -p \bmod p^2$.

Then $b\in\mathbb{Z}^+(p)$ and $pb\leqslant r+2p\leqslant(r+2)p\leqslant v_0$.

Take $v=pb$ and consider

$$\bar{\mathcal{F}}_v^{(v)}=pb\bar\Delta_{b1}-\sum a_1[\bar\Delta_{a_10},\bar\Delta_{a_20}] \bmod (\bar L_{triv}^{(v)}+p^2\bar L_W),$$

where the sum is taken for all $a_1,a_2\in\mathbb{Z}^+(p)$ such that $a_1+a_2=pb$ and $a_1>a_2$. Consider

$$\bar F_W(\bar{\mathcal{F}}_v^{(v)}) \bmod \bar L_{triv}^{(v)}+p^2\bar L_W.$$

By inductive assumption, the expression of

$$\bar F_W(p\bar\Delta_{b1}) \bmod \bar L_{triv}^{(v)}+p^2\bar L_W$$

does not contain (with non-zero coefficient) the term $p\bar\Delta_{b+r/p,1}$ (because $r/p<r$ and $\alpha_b(r/p)=0$). Therefore, the terms of $\bar{\mathcal{F}}_{v+r}^{(v)}$ does not enter into the expression of the element

$$\bar F_W(\bar{\mathcal{F}}_v^{(v)}) \bmod \bar L_{triv}^{(v)}+p^2\bar L_W.$$

On the other hand, if we follow the terms of this image in the form $[\bar\Delta_{b_10},\bar\Delta_{b_20}]$, where $b_1+b_2=v+r$, we obtain

$$-\sum_{\substack{a_1+a_2=v\\ v>a_1>a_2\geqslant 1}}\left(a_1\alpha_{a_1}(r)[\bar\Delta_{a_1+r,0},\bar\Delta_{a_20}]+a_1\alpha_{a_2}(r)[\bar\Delta_{a_10},\bar\Delta_{a_2+r,0}]\right)\equiv$$

$$2X\sum_{\substack{b_1+b_2=v+r\\ v>b_1>b_2\geqslant 1}} b_1[\bar\Delta_{b_10},\bar\Delta_{b_20}] \bmod \bar L_{triv}^{(v)}+p^2\bar L_W.$$

The right-hand sum is not empty, because $r<v=pb$ by the choice of b. Therefore, $X=0$. This proves the case $r\equiv 0 \bmod p$.

The proposition is completely proved.

3.8. Now we can finish the proof of the Main Lemma.

As we have already noted, the part a) follows from Proposition of n.3.7.

Take $v=2v_0/p$, then $v\in\mathbb{N}$, $v\equiv 0 \bmod p$ and

$$\bar{\mathcal{F}}_v^{(v)}\equiv\sum a_1[\bar\Delta_{a_10},\bar\Delta_{a_20}] \bmod \bar L_{triv}^{(v)}+p\bar L_W,$$

where the sum is taken for all $a_1,a_2\in\mathbb{Z}^+(p)$ such that $a_1+a_2=v$, $1\leqslant a_2<v_0/p$ and $v_0/p<a_1<v$.

The terms of the form $[\bar\Delta_{b_10},\bar\Delta_{b_2,m}]$, where $b_2<v_0/p$ and $m\not\equiv 0 \bmod N_0$, from the image $\bar F_W(\bar{\mathcal{F}}_v^{(v)})$ modulo $\bar L_{triv}^{(v)}+p\bar L_W$ can be written in the following way

$$\sum a_1\alpha_{a_2b_2m}[\bar\Delta_{a_10},\bar\Delta_{b_2m}],$$

where the sum is taken for all $a_1, a_2, b_2 \in \mathbb{Z}^+(p)$ such that $a_1 + a_2 = v$, $1 \leqslant a_2 < b_2 < v_0/p$ and $v_0/p < a_1 < v$.

Because $m \not\equiv 0 \bmod N_0$, we have

$$\gamma(b_2, m, a_1, 0) \leqslant b_2 + \frac{a_1}{p} < v.$$

Therefore, if $\alpha_{a_2,b_2,-m} \neq 0$, then $\gamma(a_1, 0, b_2, -m) = a_1 + b_2/p^{\hat{m}} > v$, i.e. $b_2/p^{\hat{m}} > a_2$. This gives the part b) of the main lemma.

The part c) follows now from Proposition 3 of n.2.4.

The Main Lemma is proved.

4. Fundamental exact sequence.

4.1. Let $[K : \mathbb{Q}_p] < \infty$, choose uniformiser $\pi_K \in K$ and a sequence $\{\pi_s\}_{s \geqslant 0} \subset \bar{K}$ such that $\pi_0 = \pi_K$ and $\pi_s^p = \pi_{s-1}$ for $s \in \mathbb{N}$. Set $K_s = K(\pi_s)$ and denote by $\widetilde{K}$ the union of all K_s.

We note that $\widetilde{K}$ is an APF-extension of K (we use the terminology and constructions from [Wi]), so one can apply the Fontaine-Wintenberger field-of-norms functor $\mathcal{X}$ to obtain the field $\mathcal{K} = \mathcal{X}(\widetilde{K})$. This is a complete discrete valuation field, its residue field canonically identified with the residue field k of K, and it has specific uniformiser t obtained from the above sequence $\{\pi_s\}_{s \geqslant 0}$. The functor $\mathcal{X}$ induces equivalence of the category of extensions of $\widetilde{K}$ in $\bar{K}$ and the category of extensions of $\mathcal{K}$ in $\mathcal{K}_{\mathrm{sep}} = \mathcal{X}(\bar{K})$. This gives identification

$$\mathcal{G}_{\mathcal{K}} = \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K}) = \mathrm{Gal}(\bar{K}/\widetilde{K}),$$

so we have the embedding $\iota : \mathcal{G}_{\mathcal{K}} \longrightarrow \Gamma_K$. This embedding is compatible with ramification filtrations, i.e.

$$\iota(\mathcal{G}_{\mathcal{K}}^{(x)}) = \iota(\mathcal{G}_{\mathcal{K}}) \cap \Gamma_K^{(\varphi_{\widetilde{K}/K}(x))}$$

for all $x \geqslant 0$, where $\varphi_{\widetilde{K}/K}(x)$ is the Herbrandt function of the infinite extension $\widetilde{K}/K$ (by definition $\varphi_{\widetilde{K}/K}(x) = \lim_{s \to \infty} \varphi_{K_s/K}(x)$, we note also that $\varphi_{\widetilde{K}/K}(x) = \varphi_{K_s/K}(x)$ for $x \leqslant ep^{s+1}/(p-1)$).

4.2. Assume that a primitive root of degree p^M of unity ζ_M belongs to K. Then

$$\mathrm{Gal}(K_M/K) = \mathbb{Z}/p^M\mathbb{Z}\tau_0,$$

where $\tau_0 \in \mathrm{Gal}(K_M/K)$ is uniquely characterised by the property $\tau_0(\pi_M) = \zeta_M \pi_M$.

The ramification subgroup $\Gamma_K(p)^{(a_K)}$ (where $a_K = e_K(p/(p-1) + M)$, cf. Introduction) belongs to the kernel of the natural projection

$$\Gamma_K(p) \longrightarrow \mathrm{Gal}(K_M/K),$$

because $a_K = v(K_{M+1}/K) > v(K_M/K)$.

On the other hand, the embedding ι from n.4.1 induces the homomorphism $\iota(p) : \mathcal{G}_{\mathcal{K}}(p) \longrightarrow \Gamma_K(p)$ and for $v_K = e_K p^{M+1}/(p-1)$, we have

$$\iota(p)\left(\mathcal{G}_{\mathcal{K}}(p)^{(v_K)}\right) \subset \Gamma_K(p)^{(a_K)}$$

(because $\varphi_{\widetilde{K}/K}(v_K) = a_K$).

As a result of the above considerations we obtain the following sequence of morphisms of profinite groups

$$(1) \qquad 1 \longrightarrow \mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(v_K)} \longrightarrow \Gamma_K(p)/\Gamma_K(p)^{(a_K)} \longrightarrow \mathbb{Z}/p^M\mathbb{Z}\tau_0 \longrightarrow 0.$$

Proposition. *The sequence* (1) *is exact.*

Proof.

Lemma 1. $\Gamma_K^{(a_K)} = \Gamma_{K_M}^{(v_K)}$.

Proof of lemma. We have

$$\bar{K}^{\Gamma_K^{(a_K)}} = \bigcup_{\alpha \in \mathcal{A}} L_\alpha,$$

where $\{L_\alpha\}_{\alpha\in\mathcal{A}}$ is the family of finite extensions of K in $\bar{K}$ such that $v(L_\alpha/K) < a_K$. Because

$$v(K_M/K) = e_K\left(\frac{p}{p-1} + M - 1\right) < a_K$$

we have

$$\bigcup_{\alpha\in\mathcal{A}} L_\alpha = \bigcup_{\alpha\in\mathcal{A}_1} L_\alpha,$$

where $\mathcal{A}_1 = \{\alpha \in \mathcal{A} \mid L_\alpha \supset K_M\}$. From the composition property for Herbrandt's functions $\varphi_{L_\alpha/K}(x) = \varphi_{K_M/K}\left(\varphi_{L_\alpha/K_M}(x)\right)$ and interpretation of upper ramification number $v(L_\alpha/K)$ as the second coordinate of the maximal edge point of the graph of the function $\varphi_{L_\alpha/K}$, it follows

$$v(L_\alpha/K) = \max\left\{\varphi_{K_M/K}(v(L_\alpha/K_M)), v(K_M/K)\right\}.$$

Therefore, for any $\alpha \in \mathcal{A}_1$, it holds

$$v(L_\alpha/K) < a_K \iff v(L_\alpha/K_M) < v_K$$

(because $v(K_M/K) < a_K$ and $\varphi_{K_M/K}(v_K) = a_K$). Therefore,

$$\bigcup_{\alpha\in\mathcal{A}_1} L_\alpha = \bar{K}^{\Gamma_{K_M}^{(v_K)}}$$

and $\Gamma_K^{(a_K)} = \Gamma_{K_M}^{(v_K)}$. The lemma is proved.

The above lemma gives a natural exact sequence

$$1 \longrightarrow \Gamma_{K_M}/\Gamma_{K_M}^{(v_K)} \longrightarrow \Gamma_K/\Gamma_K^{(a_K)} \longrightarrow \mathrm{Gal}(K_M/K) \longrightarrow 1$$

and, therefore, for Galois groups of corresponding maximal p-extensions $\Gamma_{K_M}(p)$ and $\Gamma_K(p)$, we obtain the exact sequence

$$1 \longrightarrow \Gamma_{K_M}(p)/\Gamma_{K_M}(p)^{(v_K)} \longrightarrow \Gamma_K(p)/\Gamma_K(p)^{(a_K)} \longrightarrow \mathrm{Gal}(K_M/K) \longrightarrow 1.$$

Clearly, our proposition is implied now by the following lemma.

Lemma 2. *The embedding $\iota : \mathcal{G}_{\mathcal{K}} \longrightarrow \Gamma_K$ induces isomorphism*

$$\bar{\iota} : \mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(v_K)} \longrightarrow \Gamma_{K_M}(p)/\Gamma_{K_M}(p)^{(v_K)}.$$

Proof. Consider the category $\mathcal{E}(K_M, v_K)$ of finite extensions L of K_M such that $v(L/K_M) < v_K$. Clearly, our lemma is implied by the following property

the correspondence $L \longrightarrow \mathcal{X}(L\widetilde{K})$ gives rise to equivalence of the category $\mathcal{E}(K_M, v_K)$ and the category $\mathcal{E}(\mathcal{K}, v_K)$ of finite extensions $\mathcal{L}$ of $\mathcal{K}$ in $\mathcal{K}_{\mathrm{sep}} = \mathcal{X}(\bar{K})$ such that $v(\mathcal{L}/\mathcal{K}) < v_K$.

We explain briefly the construction of inverse correspondence. Let $\mathcal{L} \in \mathcal{E}(\mathcal{K}, v_K)$, then $\mathcal{L} = \mathcal{X}(\widetilde{L})$, where $\widetilde{L} = L\widetilde{K}$ for some finite extension L of K. For any $s \in \mathbb{Z}_{\geqslant 0}$, set $L_s = LK_s$, then there exists an index s_0 such that $v(L_s/K_s) = v(\mathcal{L}/\mathcal{K}) < v_K$ for all $s \geqslant s_0$, cf. [Wi].

Suppose that s_0 is the minimal integer with such properties. Prove that $s_0 \leqslant M$.

Assume that $s_0 > M$, then

$$v(L_{s_0}/K_{s_0-1}) = \max\left\{\varphi_{K_{s_0}/K_{s_0-1}}(v(\mathcal{L}/\mathcal{K}), v(K_{s_0}/K_{s_0-1})\right\} =$$

$$v(K_{s_0}/K_{s_0-1}) = e_K p^{s_0}/(p-1) \geqslant v_K.$$

Therefore, the group $\Gamma_{K_{s_0-1}}^{(v(K_{s_0}/K_{s_0-1}))}$ acts nontrivially on L_{s_0}. From inequality $v(L_{s_0}/K_{s_0}) < v(K_{s_0}/K_{s_0-1})$ it follows easily that this group is of order p. Let L_{s_0-1} be the corresponding fixed subfield of L_{s_0}. Then $v(L_{s_0-1}/K_{s_0-1}) < v(K_{s_0}/K_{s_0-1})$, therefore, L_{s_0-1} and K_{s_0} are linearly disjoint over K_{s_0-1}, and it can be easily checked that $v(L_{s_0-1}/K_{s_0-1}) = v(L_{s_0}/K_{s_0})$. This gives contradiction, therefore, $s_0 \leqslant M$.

The inverse map now is defined by the correspondence $\mathcal{L} \mapsto L_M$.

The lemma and the proposition are completely proved.

4.3. Let $w_K = e_K p^M$. If $\varphi_{K_M/K}(b_K) = w_K$, where $\varphi_{K_M/K}$ is the Herbrandt function of the extension K_M/K, then the fundamental exact sequence (1) from n.4.2 induces the exact sequence

$$1 \longrightarrow \mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(w_K)} \longrightarrow \Gamma_K(p)/\Gamma_K(p)^{(b_K)} \longrightarrow \mathbb{Z}/p^M\mathbb{Z}\tau_0 \longrightarrow 0.$$

If $\hat{\tau}_0 \in \Gamma_K(p)/\Gamma_K(p)^{(b_K)}$ is a lifting of τ_0, then the conjugation by $\hat{\tau}_0$ determines the class $\mathrm{cl}(\tau_0)$ of automorphisms of the group $\mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(w_K)}$ modulo the subgroup of its inner automorphisms.

Consider a power series $P(X) \in W[[X]]$ such that $P(\pi_K) \equiv \zeta_M \bmod p$. Its essential part

$$1 + \sum_{1 \leqslant i < e_K} \alpha_i X^i = P(X) \bmod (p, X^{e_K}),$$

where all $\alpha_i \in k$, comes from uniquely defined decomposition of $\zeta_M \bmod p$ in powers of $\pi_K \bmod p$ with coefficients from k. We note that

$$P(X)^{p^M} \equiv 1 \bmod (p, X^{e_K}).$$

Set $P_M(X) = P(X)^{p^M}$ and consider $\tau_P \in \mathrm{Aut}^1 \mathcal{K}$ such that $\tau_P(t) = tP_M(t)$. We note that τ_P induces an automorphism of order p^M on $O_{\mathcal{K}} \operatorname{mod} t^{w_K}$.

If $\hat{\tau}_P$ is a lifting of τ_P to the group of all contonuous isomorphisms of the field $\mathcal{K}_{\mathrm{sep}}$, then the conjugation by $\hat{\tau}_P$ induces an automorphism of $\mathcal{G}_{\mathcal{K}}(p)$ and this automorphism respects the ramification filtration of $\mathcal{G}_{\mathcal{K}}(p)$. So, we obtain an automorphism of the quotient group $\mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(w_K)}$. We denote by $\mathrm{cl}(\tau_P)$ its class modulo the subgroup of inner automorphisms of this group.

Proposition. *For the above $P \in W[[X]]$, we have* $\mathrm{cl}(\tau_0) = \mathrm{cl}(\tau_P)$.

Proof.

4.3.1. Set for the simplicity $w_K = w$ and consider any finite Galois extension L of K such that $L \supset K_M$ and $v(L/K_M) < w$. In notation of n.4.2 consider $\mathcal{L} = \mathcal{X}(L\widetilde{K})$. Then $\mathcal{L}$ is a Galois extension of $\mathcal{K}$ and the functor $\mathcal{X}$ provides us with the identification $\mathrm{Gal}(\mathcal{L}/\mathcal{K}) = \mathrm{Gal}(L/K_M)$. With respect to this identification we must prove that

$$\mathrm{cl}(\tau_P)|_{\mathrm{Gal}(\mathcal{L}/\mathcal{K})} = \mathrm{cl}(\tau_0)|_{\mathrm{Gal}(L/K_M)}.$$

4.3.2. *Deligne's equivalence*, cf. [De]. Consider the triple

$$T_{\mathcal{L}} = (O_{\mathcal{L}}/t^w O_{\mathcal{L}}, m_{\mathcal{L}}/t^w m_{\mathcal{L}}, j)\,,$$

where $m_{\mathcal{L}}$ is the maximal ideal of the valuation ring $O_{\mathcal{L}}$ of $\mathcal{L}$ and $j : m_{\mathcal{L}}/t^w m_{\mathcal{L}} \longrightarrow O_{\mathcal{L}}/t^w O_{\mathcal{L}}$ is induced by the embedding $m_{\mathcal{L}} \longrightarrow O_{\mathcal{L}}$.

The family of triples coming from all finite extensions $\mathcal{L}$ of $\mathcal{K}$ such that $v(\mathcal{L}/\mathcal{K}) < w$ gives the family of objects of the category $(\operatorname{ext} \mathrm{Tr}_w \mathcal{K})^w$ introduced in [De]. This category can be characterised purely in intrinsic terms and the main result of [De] states that the functor $\mathcal{L} \mapsto T_{\mathcal{L}}$ establishes equivalence of the category $(\operatorname{ext} \mathcal{K})^w$ of extensions $\mathcal{L}/\mathcal{K}$ such that $v(\mathcal{L}/\mathcal{K}) < w$ and the category $(\operatorname{ext} \mathrm{Tr}_w \mathcal{K})^w$.

We note that the triple $T_{\mathcal{L}}$ has the group of automorphisms consisting of compatible pairs of $O_{\mathcal{K}}/t^w O_{\mathcal{K}}$-algebra automorphisms of $O_{\mathcal{L}}/t^w O_{\mathcal{L}}$ and $m_{\mathcal{L}}/t^w m_{\mathcal{L}}$. Then the group $\mathrm{Aut}^w(T_{\mathcal{L}})$ of automorphisms of $T_{\mathcal{L}}$ in the category $(\operatorname{ext} \mathrm{Tr}_w \mathcal{K})^w$ consists of equivalence classes modulo $m_{\mathcal{L}}^{w(\mathcal{L})}$ and modulo $m_{\mathcal{L}}^{w(\mathcal{L})+1}$, respectively, of those automorphisms, where $\varphi_{\mathcal{L}/\mathcal{K}}(w(\mathcal{L})) = w$ (the Herbrandt function $\varphi_{\mathcal{L}/\mathcal{K}}$ can be recovered completely from the triple $T_{\mathcal{L}}$). Then the group $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ coincides with the group

$$\mathrm{Aut}^w(T_{\mathcal{L}}/T_{\mathcal{K}}) = \{a \in \mathrm{Aut}^w(T_{\mathcal{L}}) \mid a|_{T_{\mathcal{K}}} = \mathrm{id}\}.$$

In particular, if morphism $\tau_P(T_{\mathcal{K}}) \in \mathrm{Aut}^w(T_{\mathcal{K}})$ corresponds to τ_P, then

$$\mathrm{cl}\,\tau_P|_{\mathrm{Gal}(\mathcal{L}/\mathcal{K})} = \mathrm{cl}(\tau_P(T_{\mathcal{K}}))|_{\mathrm{Aut}^w(T_{\mathcal{L}}/T_{\mathcal{K}})}.$$

4.3.3. Let $\bar{O}$ be the valuation ring of $\bar{K}$. Consider Fontaine's ring $R = \varprojlim_s (\bar{O}/p\bar{O})_s$, where $s \in \mathbb{Z}_{\geqslant 0}$ and transition morphisms from $(\bar{O}/p\bar{O})_{s+1}$ to $(\bar{O}/p\bar{O})_s$ are induced by taking p^{th} powers of elements of $\bar{O}$. The maximal ideal m_R of R can be also presented in the form $\varprojlim_s (\bar{m}/p\bar{m})_s$, where $\bar{m}$ is the maximal ideal of $\bar{O}$ and transition morphisms are also induced by taking p^{th} powers in $\bar{m}$.

If R_0 is the quotient field of R, then there exists a universal procedure identifying any value of the field-of-norms functor $\mathcal{X}$ with a suitable subfield of R_0, cf. [Wi]. In particular, we can assume that $\mathcal{K} \subset \mathcal{L} \subset R_0$ and these embeddings are compatible with action of the group $\mathcal{G}_K$ (recall that R has the natural Γ_K-module structure).

4.3.4. Consider two natural projections $\mathrm{pr}_M : R \longrightarrow (\bar{O}/p\bar{O})_M$ and $\mathrm{pr}_M : m_R \longrightarrow (\bar{m}/p\bar{m})_M$. Clearly, $\mathrm{pr}_M(t) = \pi_M$ and we have induced isomorphisms

$$\bar{\mathrm{pr}}_M : R/t^w R \simeq \bar{O}/p\bar{O}, \quad \bar{\mathrm{pr}}_M : O_{\mathcal{K}}/t^w O_{\mathcal{K}} \simeq O_{K_M}/pO_{K_M},$$

$$\widetilde{\mathrm{pr}}_M : m_R/t^w m_R \simeq \bar{m}/p\bar{m}, \quad \widetilde{\mathrm{pr}}_M : m_{\mathcal{K}}/t^w m_{\mathcal{K}} \simeq m_{K_M}/pm_{K_M}.$$

Note that all these isomorphisms are σ^{-M}-linear with respect to natural k-module structures of involved objects. We note also that $\bar{\mathrm{pr}}_M(P_M(t)) = \zeta_M \bmod p$.

So, we obtain isomorphism of triples

$$\mathrm{pr}_M : T_{\mathcal{K}} = (O_{\mathcal{K}}/t^w O_{\mathcal{K}}, m_{\mathcal{K}}/t^w m_{\mathcal{K}}, j) \simeq T_{K_M} = (O_{K_M}/pO_{K_M}, m_{K_M}/pm_{K_M}, j).$$

Consider the triple

$$\mathrm{pr}_M(T_{\mathcal{L}}) = (\bar{\mathrm{pr}}(O_{\mathcal{L}}/pO_{\mathcal{L}}), \widetilde{\mathrm{pr}}_M(m_{\mathcal{L}}/pm_{\mathcal{L}}), j).$$

This is an object of the category $(\mathrm{ext}\,\mathrm{Tr}_w\, K_M)^w$. By Deligne's equivalence (it works in any characteristics), this triple is of the form $T_{L'} = (O_{L'}/pO_{L'}, m_{L'}/pm_{L'}, j)$, where L' is a finite extension of K_M such that $v(L'/K_M) = v(\mathcal{L}/\mathcal{K})$ and $[L' : K_M] = [\mathcal{L} : \mathcal{K}]$. Because pr_M commutes with Galois action, we have $L' \subset L\widetilde{K}$. Therefore, cf. n.4.1, $L' = L$. Of course, $\mathrm{pr}_M(T_{\mathcal{L}}) = T_L$ and

$$\mathrm{pr}_M : \mathrm{Aut}^w(T_{\mathcal{L}}/T_{\mathcal{K}}) \simeq \mathrm{Aut}^w(T_L/T_K)$$

corresponds to the identification of the Galois groups of extensions $\mathcal{L}/\mathcal{K}$ and L/K given by the functor $\mathcal{X}$.

4.3.5. Denote by $\tau_0(T_{K_M})$ the automorphism of T_{K_M} coming from τ_0. then

$$\mathrm{pr}_M(\tau_P(T_{\mathcal{K}})) = \tau_0(T_{K_M}).$$

Therefore, pr_M maps $\mathrm{cl}(\tau_P(T_{\mathcal{K}}))|_{\mathrm{Aut}^w(T_{\mathcal{L}}/T_{\mathcal{K}})}$ to

$$\mathrm{cl}(\tau_0(T_{K_M}))|_{\mathrm{Aut}^w(T_L/T_{K_M})} = \mathrm{cl}(\tau_0)|_{\mathrm{Gal}(L/K_M)}.$$

The proposition is proved.

4.4. Remark. a) Proposition n.4.3 provides us with an opportunity to compute the action of τ_0 by conjugation on any quotient of the form $\mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(v)}$ with $v \leqslant w_K$. We shall apply it in Section 5 below for $\tilde{v}_K = v_K/p = e_K p^M/(p-1) < w_K$;
b) In fact, we need only to know the action of τ_0 on the maximal abelian quotient of period p of the group $\mathcal{G}_{\mathcal{K}}(p)/\mathcal{G}_{\mathcal{K}}(p)^{(\tilde{v}_K)}$. In this case the above proposition can be proved "by hands" by the use of the Artin-Schreier equations $T^p - T = \alpha t^{-a}$ in the characteristics p case, and the analogues of those $T^p - T = [\alpha]\pi_M^{-a}$ in the characteristics 0 case (here $\alpha \in k$, $[\alpha] \in K$ is its Teichmuller representative, $1 \leqslant a < e_K p^M$ and $(a, p) = 1$).

5. Proof of the Theorem.

5.1. Prove first that the simplest invariants of the fields K and K' coincide.

Proposition. *$f_K = f_{K'}$, $e_K = e_{K'}$ and $\zeta_M \in K'$.*

Proof. The isomorphism F induces isomorphism of corresponding maximal abelian quotients and when restricted to the subgroup $\Gamma_K(p)^{(1)} \operatorname{mod} \Gamma_K(p)^{(a_K)}$ induces isomorphism of multiplicative groups

$$F_{\mathrm{ab}}^{(1)} : U_K^{(1)} \operatorname{mod} U_K^{(a_K)} \longrightarrow U_{K'}^{(1)} \operatorname{mod} U_{K'}^{(a_K)},$$

where we use the notation $U_K^{(n)}$ (resp., $U_{K'}^{(n)}$) for the group of principal units in K (resp., K') congruent to 1 modulo n^{th} power of maximal ideal. Clearly, for $1 \leqslant n \leqslant a_K$, the morphism $F_{\mathrm{ab}}^{(1)}$ respects "ramification filtration"

$$F_{\mathrm{ab}}^{(1)} \left(U_K^{(n)} \operatorname{mod} U_K^{(a_K)} \right) = U_{K'}^{(n)} \operatorname{mod} U_{K'}^{(a_K)}.$$

This gives $f_K = f_{K'}$, because $a_K \geqslant 2$.

The followinmg two statements are standard facts about the structure of the multiplicative group of principal units:
a) if $a \in \mathbb{N}$ and $a > e_K^* := e_K p/(p-1)$, then $(U_K^{(a-e)})^p = U_K^{(a)}$;
b) the properties
— b_1) there exists $n \in \mathbb{N}$ such that $n \equiv 0 \operatorname{mod} p$ and

$$U_K^{(n)} \operatorname{mod} U_K^{(n+1)} \not\subset U_K^{(1)p} \operatorname{mod} U_K^{(n+1)},$$

— b_2) $n = e_K^*$ and $\zeta_1 \in K$,
are equivalent.

Because $\zeta_M \in K$, $a_K > e_K^*$ and $F_{\mathrm{ab}}^{(1)}$ respects "ramification filtration", we obtain

$$U_{K'}^{(e_K^*)} \operatorname{mod} U_{K'}^{(e_K^*+1)} \not\subset U_{K'}^{(1)p} \operatorname{mod} U_{K'}^{(e_K^*+1)},$$

and therefore, $e_K^* = e_{K'}^*$ or $e_{K'} = e_K$.

Finally, if $F_{\mathrm{ab}}^{(1)} \left(\zeta_M \operatorname{mod} U_K^{(a_K)} \right) = \xi \operatorname{mod} U_{K'}^{(a_K)}$, where $\xi \in U_{K'}^{(1)}$, then $\xi^{p^{M-1}} \notin U_{K'}^{(a_K)}$ but $\xi^{p^M} \in U_{K'}^{(a_K)}$. Because $U_{K'}^{(a_K)} = U_{K'}^{(e_K^*)p^M}$, we conclude that $\xi \equiv \zeta'_M \operatorname{mod} U_{K'}^{(e_K^*)}$, where ζ'_M is a primitive root of unity of degree p^M. In particular, $\zeta_M \in K'$.

The proposition is proved.

Remark. The above proposition implies that $\mathbb{Z}_p$-algebras $O_K \operatorname{mod} p^{1/(p-1)}$ and $O_{K'} \operatorname{mod} p^{1/(p-1)}$ are isomorphic. If $M = 1$, this gives already the assertion of our theorem. So, we can assume below that $M \geqslant 2$. In particular, we shall use later that $v_K \equiv 0 \operatorname{mod} p^2$.

5.2. By the above n.5.1, we can set $a_0 = a_K = a_{K'}$, $v_0 = v_K = v_{K'}$, $e = e_K = e_{K'}$ and $e^* = e_K^* = e_{K'}^*$.

In the notation of Section 4 fix uniformising element $\pi_K \in K$, the sequence $\{\pi_s\}_{s \geqslant 0} \subset \bar{K}$ and consider corresponding fundamental sequence

$$1 \longrightarrow \mathcal{G}(p)/\mathcal{G}(p)^{(v_0)} \xrightarrow{i} \Gamma(p)/\Gamma(p)^{(a_0)} \xrightarrow{j} \mathrm{Gal}(K^{(M)}/K) \longrightarrow 1$$

(where we set $\mathcal{G}_K = \mathcal{G}$ and $\Gamma_K = \Gamma$).

Proposition. *The isomorphism F transforms the fundamental exact sequence* (3) *to some fundamental exact sequence for the field K'.*

Proof. First, we note that F transforms the above fundamental sequence to the following exact sequence

$$1 \longrightarrow \mathrm{Ker}(F^{-1}\circ j) \longrightarrow \Gamma_{K'}(p)/\Gamma_{K'}(p)^{(a_0)} \longrightarrow \mathrm{Coker}(i\circ F) \longrightarrow 1.$$

Therefore, $\mathrm{Coker}(i\circ F)=\mathrm{Gal}(E/K')$ for some cyclic extension E of K' of degree p^M. So, $E=K'(\alpha^{1/p^M})$ for some $\alpha\in K'^*$, and it is sufficient to prove that

$$\alpha\notin U_{K'}^{(1)} \bmod K'^{*p^M}. \tag{2}$$

But the compatibility of F with ramification filtrations implies that all ramification jumps of the extension E/K' are the same as of the extension K_M/K. In particular, if E_1 is the unique subextension of E of degree p over K', then $v(E_1/K')=e^*$. This implies already the property (2). The proposition is proved.

5.3. In this section we put together all necessary information about the fields K and K'.

5.3.1. *The field K.* Its algebraic closure $\bar K$ is assumed to be chosen, we also fix its uniformising element π_K, a sequence $\{\pi_s\}_{s\geqslant 0}\subset\bar K$, cf. n.4.1, and a primitive root $\zeta_M\in K$ of unity of degree p^M.

To the above data we have assigned the following objects:

— the field $\mathcal K=k((t))$, where k is the residue field of K and t is a fixed uniformiser (related to the sequence $\{\pi_s\}_{s\geqslant 0}$);

— the group $\bar{\mathcal G}=\mathcal G_{\mathcal K}/\mathcal G_{\mathcal K}^{p^3}C_3(\mathcal G_{\mathcal K})$, where $\mathcal G_{\mathcal K}=\mathrm{Gal}(\mathcal K_{\mathrm{sep}}/\mathcal K)$ (and $\mathcal K_{\mathrm{sep}}$ is canonically defined by $\bar K$), together with induced ramification filtration $\{\bar{\mathcal G}^{(v)}\}_{v\geqslant 1}$;

— the k-module $\mathcal M_k^{(1)}=\mathcal M^{(1)}\otimes k$, where $\mathcal M^{(1)}=\bar{\mathcal G}^{(1)} \bmod \bar{\mathcal G}^pC_2(\bar{\mathcal G})$, together with its fixed k-basis

$$\mathcal D^{(1)}(t) \bmod p=\{D_{an}\mid a\in\mathbb Z^+(p), n\in\mathbb Z \bmod N_0\};$$

— the k-linear automorphism $m\mapsto\tau_0*m$ of $\mathcal M_k^{(1)}$ commuting with Frobenius morphism σ (induced by conjugation of any lifting $\hat\tau_0$ of $\tau_0\in\mathrm{Gal}(K_M/K)$ on $\mathcal G_{\mathcal K}(p) \bmod \mathcal G_{\mathcal K}(p)^{(v_0)}$, where $\tau_0(\pi_M)=\zeta_M\pi_M$).

5.3.2. *The field K'.* We assume that $K'\subset\bar K$, its residue field coincide with that of K, we fix a uniformiser $\pi_{K'}$ of K', the corresponding sequence $\{\pi'_s\}_{s\geqslant 0}$ and a primitive root $\zeta'_M\in K'$ of degree p^M of unity.

Then we relate to the field K' the objects similar to objects related to the field K in the above n.5.3.1. The notation for objects related to K' is obtained from the corresponding notation for objects related to K by adding a stroke.

5.3.3. The above data introduced for the fields K and K' are related in the following way:

— there exists isomorphism $\bar G:\bar{\mathcal G}\longrightarrow\bar{\mathcal G}'$ such that $\bar G(\bar{\mathcal G}^{(v)})=\bar{\mathcal G}'^{(v)}$ for all $1\leqslant v\leqslant v_0$ (this property is equivalent to the existence of the isomorphism of the quotients $\bar{\mathcal{G}}/\bar{\mathcal{G}}^{(v_0)}$ and $\bar{\mathcal{G}}'/\bar{\mathcal{G}}'^{(v_0)}$ compatible with ramification filtrations because $\bar{\mathcal{G}}$ and $\bar{\mathcal{G}}'$ are characteristical quotients of free pro-p-groups);

— if $g = \bar{G} \bmod \bar{\mathcal{G}}^p C_2(\bar{\mathcal{G}})$ and $g_k = g \otimes k : \mathcal{M}_k^{(1)} \longrightarrow \mathcal{M}'^{(1)}_k$, then for any $a \in \mathbb{Z}^+(p)$ and $m \in \mathcal{M}_k^{(1)}$, we have

$$g_k(\tau_0 * m) \equiv \tau_0' * g_k(m) \bmod \mathcal{M}'^{(v_0)}_k.$$

5.4. For $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \bmod N_0$, consider $C_{an} = g_k^{-1}(D'_{an})$. Then the set

$$\{C_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\}$$

creates a k-basis of $\mathcal{M}_k^{(1)}$ satisfying the conditions a) and b) from n.1.6. Therefore, there exist $n_0 \in \mathbb{Z} \bmod N_0$ and uniformising element $\tilde{t}$ of the field $\mathcal{K}$ such that in terms of the special basis $\mathcal{D}^{(1)}(\tilde{t}) = \{\widetilde{D}_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \bmod N_0\}$ we have for all $a \in \mathbb{Z}^+(p)$,

$$\sigma^{n_0} C_{a0} = \sum_{\substack{b \in \mathbb{Z}^+(p) \\ m \in \mathbb{Z} \bmod N_0}} \alpha_{abm} \widetilde{D}_{bm},$$

where all coefficients $\alpha_{abm} \in k$, $\alpha_{110} = 1$, $\alpha_{1b0} = 0$ for all $b \in \mathbb{Z}^+(p), b > 1$, and $\alpha_{2b0} = 0$ for all $b \equiv 1 \bmod p$.

Consider the fields isomorphism $h : \mathcal{K} \longrightarrow \mathcal{K}'$ such that $h(\tilde{t}) = t'$ and $h|_k = \sigma^{-n_0}$ (recall that the residue fields of $\mathcal{K}$ and $\mathcal{K}'$ are identified with that of K). Clearly, h gives a compatible with ramification fitrations isomorphism H from $\mathcal{G}$ to $\mathcal{G}'$. Therefore, we obtain the induced isomorphism $\bar{H} : \bar{\mathcal{G}} \longrightarrow \bar{\mathcal{G}}'$ and the k-linear isomorphism $h_k : \mathcal{M}_k^{(1)} \longrightarrow \mathcal{M}'^{(1)}_k$ such that $h_k(\widetilde{D}_{an}) = \sigma^{n_0} D'_{an}$ for all $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \bmod N_0$.

Consider the group automorphism

$$\bar{F} = \bar{H} \circ \bar{G}^{-1} : \bar{\mathcal{G}} \longrightarrow \bar{\mathcal{G}},$$

then for the corresponding k-linear map $f_k : \mathcal{M}_k^{(1)} \longrightarrow \mathcal{M}_k^{(1)}$, we have $f_k(\widetilde{D}_{an}) = \sigma^{n_0} C_{an} := \widetilde{C}_{an}$.

Because $\bar{F}$ respects ramification filtration and by the above special choice of the special basis $\mathcal{D}^{(1)}(\tilde{t})$, we can apply the Main Lemma from n.3, cf. Remark n.5.1. This gives the existence of $\beta_{c,-m} \in k$, where $c \in \mathbb{Z}^+(p)$ and $1 \leqslant m < N_0$, such that for $a \in \mathbb{Z}^+(p)$, $a < \tilde{v}_0 = v_0/p = ep^M/(p-1)$, we have

$$\widetilde{C}_{a0} = \widetilde{D}_{a0} + \sum_{c,m} \beta_{c,-m} \widetilde{D}_{ap^m+c,-m} \bmod \mathcal{M}_k^{(\tilde{v}_0)}.$$

Remark. We agree to use the same notation for residue $m \in \mathbb{Z} \bmod N_0$ and for its lifting from the interval $[0, N_0)$.

Lemma. *For $c \in \mathbb{Z}^+(p)$ and $1 \leqslant m < N_0$, there exist $\gamma_{c,-m} \in k$ such that for $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$, it holds*

$$\widetilde{D}_{a0} = \widetilde{C}_{a0} + \sum_{c,m} \gamma_{c,-m} \widetilde{C}_{ap^m+c,-m} \bmod \mathcal{M}_k^{(\tilde{v}_0)}.$$

Proof. It is easy to see that these elements $\gamma_{c,-m}$ can be found uniquely from the following equations

$$0 = \beta_{c,-m} + \gamma_{c,-m} + \sum \gamma_{c_1,-m_1}\sigma^{-m_1}(\beta_{c_2,-m_2}),$$

where the sum is taken for $c_1, c_2 \in \mathbb{Z}^+(p)$ and $m_1, m_2 \in \mathbb{Z} \bmod N_0$ such that $c_1 p^{m_2} + c_2 = c$, $m_1 + m_2 = m$ and $m_2 \neq 0$.

5.5. For $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$, set

$$\varepsilon_a = 1 + \sum_{c,m} \tilde{t}^c \sigma^m(\gamma_{c,-m}),$$

where the sum is taken for natural numbers m and $c < a$ such that $v_p(a - c) = m$ (v_p is the p-adic valuation such that $v_p(p) = 1$).

Choose a power series $P = P(X) \in W[[X]]$ such that $P(\pi_K) \equiv \zeta_M \bmod p$. As in n.4.3 consider $\tau_P \in \mathrm{Aut}^1 \mathcal{K}$ such that $\tau_P(t) = tP_M(t)$, where $P_M(X) = P(X)^{p^M}$.

Proposition. *In the above notation we have the following congruence*

$$\sum \tilde{t}^{-a}\varepsilon_a(\tau_0 * \widetilde{C}_{a0}) \equiv \sum \tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a)\widetilde{C}_{a0} \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}},$$

where the sum is taken for all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$.

Proof. By n.1.5, we have

$$\sum \tilde{t}^{-a}(\tau_P * \widetilde{D}_{a0}) \equiv \sum (\tau_P^{-1}\tilde{t})^{-a}\widetilde{D}_{a0} \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}},$$

where the sum is taken for $a \in \mathbb{Z}^+(p)$.

By n.4.3, we have $\tau_P * \widetilde{D}_{a0} = \tau_0 * \widetilde{D}_{a0}$ for all $a \in \mathbb{Z}^+(p) \cap [1, ep^M)$.

By the use of the formula from Lemma n.5.4, we obtain the congruence

$$\sum_{a\in\mathbb{Z}^+(p)} \tilde{t}^{-a}(\tau_0 * \widetilde{D}_{a0}) \equiv \sum_{a\in\mathbb{Z}^+(p)} \tilde{t}^{-a}(\tau_0 * \widetilde{C}_{a0}) +$$

$$+ \sum_{\substack{a,c\in\mathbb{Z}^+(p)\\ m\in\mathbb{N}}} \tilde{t}^{-ap^m}\sigma^m(\gamma_{c,-m})(\tau_0 * \widetilde{C}_{ap^m+c,0})$$

$$\equiv \sum_{a\in\mathbb{Z}^+(p)} \tilde{t}^{-a}\varepsilon_a(\tau_0 * \widetilde{C}_{a0}) \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}} + \mathcal{M}^{(\tilde{v}_0)} \otimes \mathcal{K}.$$

Similarly,

$$\sum_{a\in\mathbb{Z}^+(p)} (\tau_P^{-1}\tilde{t})^{-a}\widetilde{D}_{a0} \equiv \sum_{a\in\mathbb{Z}^+(p)} \tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a)\widetilde{C}_{a0} \bmod (\sigma - \mathrm{id})\mathcal{M}_{\mathcal{K}} + \mathcal{M} \otimes O_{\mathcal{K}} + \mathcal{M}^{(\tilde{v}_0)} \otimes \mathcal{K}.$$

The proposition is proved.

5.6. Consider $P'(X)\in W[[X]]$ such that $P'(\pi_{K'})\equiv\zeta'_M \operatorname{mod} p$. Set $P'_M(X)=P'(X)^{p^M}$, and consider $\tau_{P'}\in \operatorname{Aut}^1\mathcal{K}'$ such that $\tau_{P'}(t')=t'P'_M(t')$. For $a\in\mathbb{Z}_{\geqslant 0}$, set

$$P'_M(X)^a \operatorname{mod} p=\sum_{i\geqslant 0}A_i'^{(a)}X^{ip^M},$$

where all coefficients $A_i'^{(a)}\in k$. We note, that

$$P'_M(X)^{p^M}\equiv 1 \operatorname{mod}(p, X^{ep^M})$$

and, therefore, for all $a\in[p^M, ep^M)$, we have $A_i'^{(a-p^M)}=A_i'^{(a)}$ (we note also that $A_0'^{(a)}=1$, $A_i'^{(a)}=0$ if $0<i<e/(p-1)$, and $A_{e/(p-1)}'^{(a)}\neq 0$).

Proposition. *For all $a\in\mathbb{Z}^+(p)\cap[1,ep^M)$, we have*

$$\tau_0*\widetilde{C}_{a0}=\sum_{i\geqslant 0}\sigma^{n_0}(A_i'^{(a)})\widetilde{C}_{a+ip^M,0} \operatorname{mod}\mathcal{M}_k^{(ep^M)}.$$

Proof. By nn.4.3 and 1.5, we have

$$\sum_{a\in\mathbb{Z}^+(p)}\tau_{P'}^{-1}(t'^{-a})D'_{a0}\equiv\sum_{a\in\mathbb{Z}^+(p)}t'^{-a}(\tau_0'*D'_{a0}) \operatorname{mod}(\sigma-\mathrm{id})\mathcal{M}'_{\mathcal{K}'}+\mathcal{M}'\otimes O_{\mathcal{K}'}+\mathcal{M}'^{(ep^M)}\otimes\mathcal{K}.$$

This gives

$$\tau_0'*D'_{a0}\equiv\sum_{i\geqslant 0}A_i'^{(a)}D'_{a+ip^M,0} \operatorname{mod}\mathcal{M}_k'^{(ep^M)}.$$

It remains only to note that

$$g_k(\tau_0*C_{a0})\equiv\tau_0'*D'_{a0} \operatorname{mod}\mathcal{M}_k^{(v_0)},$$

cf. n.5.3.3, and $\widetilde{C}_{a0}=\sigma^{n_0}C_{a0}$.

5.7. Propositions of nn.5.5 and 5.6 give the following congruence

$$\sum_a\tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a)\widetilde{C}_{a0}\equiv\sum_{a,i}\tilde{t}^{-a+ip^M}\sigma^{n_0}(A_i'^{(a)})\varepsilon_{a-ip^M}\widetilde{C}_{a0} \operatorname{mod}(\sigma-\mathrm{id})\mathcal{M}_{\mathcal{K}}+\mathcal{M}\otimes O_{\mathcal{K}},$$

where a runs over the set $\mathbb{Z}^+(p)\cap[1,\tilde{v}_0)$ and i runs over $\mathbb{Z}_{\geqslant 0}$.

Because $p^{N_0}>\tilde{v}_0$, this gives for all $a\in\mathbb{Z}^+(p)\cap[1,\tilde{v}_0)$, that

$$\tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a)\equiv\sum_{i\geqslant 0}\tilde{t}^{-a+ip^M}\sigma^{n_0}(A_i'^{(a)})\varepsilon_{a-ip^M} \operatorname{mod} O_{\mathcal{K}}. \tag{3}$$

Lemma. *For all $a \in \mathbb{Z}^+(p) \cap (p^M, \tilde{v}_0)$, it holds*

$$\tilde{t}^{-a}\varepsilon_{a-p^M} \equiv \tilde{t}^{-a}\varepsilon_a \bmod \sigma^M \mathcal{K}.$$

Proof follows immediately from the definition of ε_a, cf. n.5.5.

Now the congruence (3) gives for all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$

$$\tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a) \equiv \tilde{t}^{-a}\varepsilon_a(\sigma_*^{n_0} P'_M)(\tilde{t})^a \bmod (\sigma^M \mathcal{K} + O_{\mathcal{K}}), \tag{4}$$

where the power series $\sigma_*^{n_0} P'_M$ is obtained from the power series P'_M by applying σ^{n_0} to all its coefficients.

5.8. For $m \in \mathbb{Z} \bmod p^M$, denote by $\mathcal{N}_m$ the k-submodules of $t^{-(\tilde{v}_0-1)}O_{\mathcal{K}}$ generated by elements of the set

$$\{t^{-a} \mid a \in \mathbb{N} \cap [1, \tilde{v}_0), a \bmod p^M = m\}.$$

Clearly, these modules are τ_P-invariant and

$$t^{-(\tilde{v}_0-1)}O_{\mathcal{K}} \bmod O_{\mathcal{K}} = \bigoplus_{m \in \mathbb{Z} \bmod p^M} \mathcal{N}_m.$$

For $m \in \mathbb{Z} \bmod p^M$, denote by pr_m the projection from $t^{-(\tilde{v}_0-1)}O_{\mathcal{K}} \bmod O_{\mathcal{K}}$ to $\mathcal{N}_m$. Clearly, if $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and $m = a \bmod p^M$, then

$$\mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a) = t^{-a}\sigma^M b_a \bmod O_{\mathcal{K}},$$

where $b_a \in O_{\mathcal{K}}^*$. In this notation we have

$$\mathrm{pr}_m(\tau_P^{-1}(\tilde{t}^{-a}\varepsilon_a) \bmod O_{\mathcal{K}}) = \tau_P^{-1}(\mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a) \bmod O_{\mathcal{K}}) = t^{-a}(\sigma^M b)P_M(t)^a \bmod O_{\mathcal{K}}.$$

On the other hand,

$$\begin{aligned}\mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a(\sigma_*^{n_0}P'_M)(\tilde{t})^a \bmod O_{\mathcal{K}}) &= \mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a)(\sigma_*^{n_0}P'_M)(\tilde{t})^a \bmod O_{\mathcal{K}} \\ &= t^{-a}(\sigma^M b_a)(\sigma_*^{n_0}P'_M)(\tilde{t})^a \bmod O_{\mathcal{K}}.\end{aligned}$$

Therefore, the congruence (4) gives

$$t^{-a}P_M(t)^a \equiv t^{-a}(\sigma_*^{n_0}P'_M)(\tilde{t})^a \bmod O_{\mathcal{K}}.$$

By taking $a = \tilde{v}_0 - 1$, we obtain from this congruence that

$$P_M(t) \equiv (\sigma_*^{n_0}P'_M)(\tilde{t}) \bmod t^{\tilde{v}_0-1}O_{\mathcal{K}},$$

and finally

$$P(t) \equiv (\sigma_*^{n_0}P')(\tilde{t}) \bmod t^{e/(p-1)}O_{\mathcal{K}}.$$

Let $\theta(X) \in W[[X]]$ be such that $t = \theta(\tilde{t})$. Consider $\widetilde{P}(X) = P(\theta(X)) \in W[[X]]$. Then $P(t) = \widetilde{P}(\tilde{t})$ and we obtain the relation

$$\widetilde{P}(\tilde{t}) \equiv (\sigma_*^{n_0})P'(\tilde{t}) \bmod t^{e/(p-1)}O_{\mathcal{K}}.$$

Introduce new uniformiser $\tilde{\pi}_K \in K$ by the relation $\pi_K = \theta(\tilde{\pi}_K)$, then $\widetilde{P}(\tilde{\pi}_K) \equiv \zeta_M \bmod p$, and

$$(\sigma_*^{n_0}P')(\tilde{\pi}_K) \equiv \zeta_M \bmod p^{1/(p-1)}. \tag{5}$$

On the other hand, by definition we have that

$$P'(\pi_{K'}) \equiv \zeta'_M \bmod p. \tag{6}$$

Let $\phi \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_M)/\mathbb{Q}_p)$ be such that $\phi(\zeta_M) = \zeta'_M$. Denote by $\tilde{\phi}$ the isomorphism from $O_K \bmod p^{1/(p-1)}$ to $O_{K'} \bmod p^{1/(p-1)}$ uniquely determined by conditions $\tilde{\phi}(\tilde{\pi}_K) = \pi_{K'}$ and $\tilde{\phi}|_k = \sigma^{-n_0}$. Then the above formulae (5) and (6) imply that $\tilde{\phi}$ is a ϕ-linear isomorphism of $\mathbb{Z}_p[\zeta_M]$-algebras.

The theorem is proved.

REFERENCES

[Ab1] V.A. Abrashkin, *Ramification filtration of the Galois group of a local field. II*, Proceeding of Steklov Math. Inst. **208** (1995).

[Ab2] V.A.Abrashkin, *Ramification filtration of the Galois group of a local field. III*, Preprint MPI 96-103 (to appear in Izvestiya RAN, ser. matem.).

[Ab3] V.A.Abrashkin, *One group-theoretic property of the ramification filtration,*, Preprint MPI 96-153 (to appear in Izvestiya RAN, ser. matem.).

[De] P.Deligne, *Les corps locaux de caracterisque p, limites de corps locaux de caracterisque 0.*, Representations des groups reductifs sur un corps local. Travaux en Cours., Paris:Hermann. 1984, p. 120-157.

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

[Ma] E.Maus, *Relationen in Verzweigungsgruppen*, J. reine ang. Math. **258** (1973), 23-50.

[Po] F. Pop, *Glimpses of Grothendieck's anabelian geometry*, London Mathematical Society, Lecture Note Series **242**, 113-126.

[Se] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968.

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

STEKLOV MATH. INSTITUTE, UL. GUBKINA 8, MOSCOW 117 966, RUSSIA
E-mail address: `victor@abrvic.mian.su`