A STRONG PROPERTY OF RAMIFICATION FILTRATION. II

Victor A. Abrashkin

For two finite extensions of the p-adic field $\mathbb{Q}_p$ in the same algebraic closure $\bar{\mathbb{Q}}_p$, where $p \geqslant 5$, it is proved that any isomorphism of their Galois groups respecting ramification filtrations comes from conjugation by some element of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. In particular, such field E can be uniquely recovered from the abstract group theoretic structure of its Galois group Γ_E together with ramification filtration $\{\Gamma_E^{(v)}\}_{v\geqslant 0}$.

0. Introduction.

Throughout all this paper p is a prime number, we assume that an algebraic closure $\bar{\mathbb{Q}}_p$ of the field of p-adic numbers $\mathbb{Q}_p$ is chosen, and if E is a finite extension of $\mathbb{Q}_p$ in $\bar{\mathbb{Q}}_p$, then we use the notation $\Gamma_E = \mathrm{Gal}(\bar{\mathbb{Q}}_p/E)$. We denote usually by $\mathbb{Z}^+(p)$ the set of natural numbers relatively prime to p.

0.1. Consider the category $\mathcal{F}_{\mathbb{Q}_p}$ of finite extensions $E/\mathbb{Q}_p$ in $\bar{\mathbb{Q}}_p$ such that for any $E_1, E_2 \in \mathcal{F}_{\mathbb{Q}_p}$, the set of morphisms $\mathrm{Hom}_{\mathcal{F}_{\mathbb{Q}_p}}(E_1, E_2)$ consists of $\tau \in \Gamma_{\mathbb{Q}_p}$ such that $\tau(E_1) \subset E_2$, what is equivalent to the inclusion $\Gamma_{E_2} \subset \tau^{-1}\Gamma_{E_1}\tau$.

Let $\mathcal{P}$ be the category of profinite finitely generated groups, such that for any two its objects Γ_1 and Γ_2, $\mathrm{Hom}_{\mathcal{P}}(\Gamma_1, \Gamma_2)$ consists of continuous monomorphisms $f : \Gamma_1 \longrightarrow \Gamma_2$ such that $[\Gamma_2 : f(\Gamma_1)] < \infty$.

Consider the functor $PG : \mathcal{F}_{\mathbb{Q}_p} \longrightarrow \mathcal{P}$ such that for any $E \in \mathcal{F}_{\mathbb{Q}_p}$, $PG(E) = \Gamma_E$. This functor is very far from to be fully faithful (but in the case of the category of algebraic number fields $\mathcal{F}_{\mathbb{Q}}$ its analogue is fully faithful by the Neukirch-Uchida-Iwasawa-Ikeda theorem).

0.2. The Galois group Γ_E of $E \in \mathcal{F}_{\mathbb{Q}_p}$ has the additional structure given by its normal closed ramification subgroups $\Gamma_E^{(v)}$, $v \geqslant -1$. We note that $\Gamma_E^{(-1)} = \Gamma_E$, $\Gamma_E^{(v)} = \Gamma_E^{(0)}$ for $-1 < v \leqslant 0$, this filtration is left-continuous and has very rich structure (e.g. any positive rational number appears as a jump of this filtration).

If $\tau \in \mathrm{Hom}_{\mathcal{F}_{\mathbb{Q}_p}}(E_1, E_2)$, then τ induces the continuous group monomorphism $\tau^* : \Gamma_{E_2} \longrightarrow \Gamma_{E_1}$ (given by the correspondence $g \mapsto \tau g \tau^{-1}$ for $g \in \Gamma_{E_2}$), $[\Gamma_{E_1} : \tau^*(\Gamma_{E_2})] < \infty$, and τ^* is compatible with ramification filtrations in the following sense, for $v \geqslant 0$ one has $\tau^*(\Gamma_{E_2}) \cap \Gamma_{E_1}^{(v)} = \tau^*(\Gamma_{E_2}^{(x)})$, where $v = \varphi_{E_2/\tau(E_1)}(x)$ is Herbrand's function of the extension $E_2/\tau(E_1)$.

One can imitate the above properties of ramification filtration to define the category $\Phi\mathcal{P}$ of profinite groups with "ramification" filtration. Then for any $E \in$

The author had a nice opportunity to work on this subject during his stay at the MPI, Bonn (the spring of 1998) and expresses his gratitude to this organisation for hospitality. He is also very grateful to Prof. F.Pop for helpful discussions resulted in the essential clarification of the final statement.

$\mathcal{F}_{\mathbb{Q}_p}$, the correspondence $E \mapsto \{\Gamma_E^{(v)}\}_{v\geqslant -1}$ gives the functor $\Phi G : \mathcal{F}_{\mathbb{Q}_p} \longrightarrow \Phi\mathcal{P}$. The main result of this paper is the fully faithfulness of this functor if $p \geqslant 5$. We prove this result in the following equivalent form.

Theorem. *Let $p \geqslant 5$, $E, E' \in \mathcal{F}_{\mathbb{Q}_p}$ and let $F : \Gamma_E \longrightarrow \Gamma_{E'}$ be a continuous group isomorphism such that for all $v \geqslant 0$, $F(\Gamma_E^{(v)}) = \Gamma_{E'}^{(v)}$. Then there exists $\tau \in \Gamma_{\mathbb{Q}_p}$ such that for all $g \in \Gamma_E$, one has $F(g) = \tau^{-1} g \tau$.*

The proof of this theorem uses a slight development of arguments from [Ab], where it was shown that a field $E \in \mathcal{F}_{\mathbb{Q}_p}$ can be uniquely recovered from the group Γ_E together with some segment of its ramification filtration under the assumption that the field E contains "sufficiently many" roots of unity (i.e. if its residue field is sufficiently big and it contains a primitive root of unity of degree p^M for a sufficiently large $M \in \mathbb{N}$).

1. An auxiliary statement.

1.1. Let $K \in \mathcal{F}_{\mathbb{Q}_p}$. Denote its residue field by k and absolute ramification index by e_K. In this section we choose an algebraic closure $\bar{K}$ of K and shall use the notation $\Gamma = \Gamma_K(p)$ for the Galois group of the maximal p-extension of K in $\bar{K}$. We denote by $\{\Gamma^{(v)}\}_{v\geqslant 1}$ the ramification filtration of the group Γ in upper numbering. Suppose that $p \geqslant 5$, a primitive root ζ_M of degree p^M of unity, where $M \in \mathbb{N}$, belongs to K, and $f_K = [k : \mathbb{F}_p] \geqslant \log_p(p^2 v_K)$, where $v_K = e_K p^{M+1}/(p-1)$.

Let $a_K = e_K(p/(p-1) + M)$ and assume that for some finite extension K' of $\mathbb{Q}_p$, there exists a group isomorphism

$$G : \Gamma/\Gamma^{(a_K)} \longrightarrow \Gamma'/\Gamma'^{(a_K)},$$

which is compatible with induced ramification filtrations (here $\Gamma' = \Gamma_{K'}(p)$ is the Galois group of the maximal p-extension of K' and $\Gamma'^{(a_K)}$ is the corresponding higher ramification subgroup). Under the above assumptions we proved in [Ab] that the simplest invariants of the fields K and K' coincide (i.e. $e_K = e_{K'}$, $f_K = f_{K'}$ and $\zeta_M \in K'$) and constructed for some $\phi_M \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_M)/\mathbb{Q}_p)$, a ϕ_M-linear isomorphism of $\mathbb{Z}_p[\zeta_M]$-algebras

$$\tilde{\phi} : O_K \bmod p^{1/(p-1)} \longrightarrow O_{K'} \bmod p^{1/(p-1)}.$$

Set $f_K = N_0$, $v_K = v_0$, $e_K = e$, $a_K = a_0$ and denote by $U_K^{(a_0)}$ (resp., $U_{K'}^{(a_0)}$) the subgroup of principal units of K (resp., K') congruent to 1 modulo the a_0^{th} power of the maximal ideal of its valuation ring. Taking the group isomorphism G on the level of maximal abelian quotients and using the reciprocity map of local class field theory we obtain the group isomorphism

$$G^{\mathrm{ab}} : U_K^{(1)} \bmod U_K^{(a_0)} \longrightarrow U_{K'}^{(1)} \bmod U_{K'}^{(a_0)}.$$

We note that $e \geqslant e_{\mathbb{Q}_p(\zeta_M)} = p^{M-1}(p-1)$ and therefore, $a_0 > p^M + 1$.

Proposition. *If $M \geqslant 2$ then the isomorphism*

$$G^{\mathrm{ab}} \bmod U_K^{(1)p} U_K^{(p^M+1)} : U_K^{(1)}/U_K^{(1)p} U_K^{(p^M+1)} \longrightarrow U_{K'}^{(1)}/U_{K'}^{(1)p} U_{K'}^{(p^M+1)},$$

is induced by $\tilde{\phi}$.

Proof. The proof of this proposition is based completely on contructions from the proof of the main theorem from [Ab], which gives the existence of the above ϕ_M-linear isomorphism $\tilde{\phi}$. We start in nn.1.2-1.6 by recalling all necessary concepts and notation from its construction.

1.2. Fix an algebraic closure $\bar{K}$ of K, a primitive root ζ_M of degree p^M of unity, a uniformiser π of K and a sequence $\{\pi_s\}_{s\geqslant 0}$ of elements of $\bar{K}$ such that $\pi_{s+1}=\pi_s$ for all s and $\pi_0=\pi$. Then we have a fundamental exact sequence

$$1\longrightarrow \mathcal{G}/\mathcal{G}^{(v_0)}\xrightarrow{i}\Gamma/\Gamma^{(a_0)}\xrightarrow{j}\mathbb{Z}/p^M\mathbb{Z}\tau_0\longrightarrow 0, \tag{1}$$

where:
a) $\mathbb{Z}/p^M\mathbb{Z}\tau_0=\mathrm{Gal}(K_M/K)$ with $K_M=K(\pi_M)$ and τ_0 is uniquely determined by the condition $\tau_0\pi_M=\zeta_M\pi_M$;
b) the epimorphism j is induced by the natural projection of the Galois group Γ to $\mathrm{Gal}(K_M/K)$;
c) $\mathcal{G}$ is the Galois group of the maximal p-extension of the complete discrete valuation field $\mathcal{K}=\mathcal{X}(\widetilde{K})$ of characteristics p in its separable closure $\mathcal{K}_{\mathrm{sep}}=\mathcal{X}(\bar{K})$, where $\mathcal{X}$ is the field-of-norms functor and $\widetilde{K}=K(\{\pi_s\mid s\geqslant 0\})$. We note that the residue field of $\mathcal{K}$ is canonically identified with k and $\mathcal{K}$ has the "special" uniformiser t coming from the sequence $\{\pi_s\}_{s\geqslant 0}$;
d) the embedding i is induced by the identification $\mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})=\mathrm{Gal}(\bar{K}/\widetilde{K})$ coming from the construction of the field-of-norms functor. By standard properties of this functor the morphism i is compatible with ramification filtrations (corresponding upper ramification numbers are related via Herbrand's function of the infinite extension $\widetilde{K}/K$).

In [Ab] it was proved that the isomorphism $G:\Gamma/\Gamma^{(a_0)}\longrightarrow\Gamma'/\Gamma'^{(a_0)}$ maps the above fundamental exact sequence (1) to some fundamental exact sequence for the field K' (this field is assumed to be a subfield of $\bar{K}$). In other words, there exist a primitive root ζ'_M of degree p^M of unity, a uniformiser π' of K', a sequence $\{\pi'_s\}_{s\geqslant 0}\subset\bar{K}$ such that $\pi'_{s+1}=\pi'_s$ for all s and $\pi'_0=\pi'$, which give rise to the fundamental exact sequence for the field K'

$$1\longrightarrow \mathcal{G}'/\mathcal{G}'^{(a_0)}\xrightarrow{i'}\Gamma'/\Gamma'^{(a_0)}\xrightarrow{j'}\mathbb{Z}/p^M\mathbb{Z}\tau'_0\longrightarrow 0,$$

where $\mathcal{G}'$ is the Galois group of the maximal p-extension of $\mathcal{K}'=\mathcal{X}(\widetilde{K}')$ in $\mathcal{X}(\bar{K})$ and $\widetilde{K}'$ is a composit of all $K'(\pi'_s)$. The choice of the above data could be done to provide us with existence of two group isomorphisms $G_1:\mathcal{G}/\mathcal{G}^{(v_0)}\longrightarrow\mathcal{G}'/\mathcal{G}'^{(v_0)}$ and $G_2:\mathbb{Z}/p^M\mathbb{Z}\tau_0\longrightarrow\mathbb{Z}/p^M\mathbb{Z}\tau'_0$ such that $G_1\circ i'=i\circ G$, $j\circ G_2=G\circ j'$ and $G_2(\tau_0)=\tau'_0$ (where τ'_0 is uniquely determined by the condition $\tau'_0(\pi'_M)=\pi'_M\zeta'_M$). We note that G_1 is compatible with ramification filtrations of the Galois groups $\mathcal{G}$ and $\mathcal{G}'$. We shall denote by t' the uniformiser of the field $\mathcal{K}'$ coming from the above sequence $\{\pi'_s\}_{s\geqslant 0}$.

1.3. Consider the pro-p-group $\mathcal{K}^*/\mathcal{K}^{*p}$ as a profinite $\mathbb{F}_p$-module. Introduce k-module $\mathcal{M}_k=\mathcal{K}^*/\mathcal{K}^{*p}\otimes k$ together with its k-submodules $\mathcal{M}_k^{(a)}$, where $a\in\mathbb{N}$, generated by the images of principal units of $\mathcal{K}$ congruent to 1 modulo t^a. All these modules have the natural semilinear action of Frobenius coming from the absolute Frobenius morphism of the field k. Consider the map

$$\mathrm{pr}_k^{\mathrm{ab}} : \mathcal{G}/\mathcal{G}^{(v_0)} \longrightarrow \left(\mathcal{G}/\mathcal{G}^{(v_0)}\right)^{\mathrm{ab}} \otimes k = \mathcal{M}_k \,\mathrm{mod}\, \mathcal{M}_k^{(v_0)}$$

given by the composition of projection to maximal abelian quotient with extension of scalars. Consider the push down of the fundamental exact sequence (1) via this morphism $\mathrm{pr}_k^{\mathrm{ab}}$

$$0 \longrightarrow \mathcal{M}_k \,\mathrm{mod}\, \mathcal{M}_k^{(v_0)} \longrightarrow \mathrm{pr}_{k*}^{\mathrm{ab}}\left(\Gamma/\Gamma^{(a_0)}\right) \longrightarrow \mathbb{Z}/p^M\mathbb{Z}\tau_0 \longrightarrow 0.$$

This exact sequence provides us with a k-linear automorphism $m \mapsto \tau_0 * m$ of $\mathcal{M}_k \,\mathrm{mod}\, \mathcal{M}_k^{(v_0)}$ given by conjugation by any lifting of τ_0. The following properties come from Artin-Schreier theory and provide us with an opportunity to compute this automorphism on the k-submodule $\mathcal{M}_k^{(1)} \,\mathrm{mod}\, \mathcal{M}_k^{(v_0)}$.

a) *Existence of special bases.* Any choice of uniformising element $\tilde{t}$ of $\mathcal{K}$ gives rise to the special basis $\mathcal{D}^{(1)}(\tilde{t}) = \{\widetilde{D}_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \,\mathrm{mod}\, N_0\}$ of the k-module $\mathcal{M}_k^{(1)}$ (recall that we set $f_K = N_0$, i.e. $k \simeq \mathbb{F}_{p^{N_0}}$) . The definition of the special basis can be done as follows. Consider the identification $U_{\mathcal{K}}^{(1)} = \prod_{a \in \mathbb{Z}^+(p)} W_a$, where $W_a = W$ is the additive group of Witt vectors with coefficients in k. This identification depends only on the choice of $\tilde{t}$ and is given by the correspondence

$$u \mapsto \{w_a \mid w_a \in W, a \in \mathbb{Z}^+(p)\},$$

where $u = \prod_{(a,p)=1} E(w_a, \tilde{t}^a)$ and $E(w, X) = \exp(wX + \dots + \sigma^n(w)X^{p^n}/p^n + \dots) \in W[[X]]$. Then

$$\mathcal{M}_k^{(1)} = U_{\mathcal{K}}^{(1)} \otimes k = \prod_{a,n} (k)_{an},$$

where a runs over $\mathbb{Z}^+(p)$ and n runs over $\mathbb{Z} \,\mathrm{mod}\, N_0$. By definition, the element $\widetilde{D}_{an} \in \mathcal{M}_k^{(1)}$ of the special basis $\mathcal{D}^{(1)}(\tilde{t})$ comes from $1 \in k = (k)_{an}$.

b) *Relation between different special bases.* Let

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

be the special basis of $\mathcal{M}_k^{(1)}$ corresponding to the uniformiser t from n.1.2 c). Then the relation between elements of the special bases $\mathcal{D}^{(1)}(t)$ and $\mathcal{D}^{(1)}(\tilde{t})$ is given via the following formal congruence in $\mathcal{M}_k^{(1)} \otimes_k \mathcal{K}$

$$\sum_{a \in \mathbb{Z}^+(p)} t^{-a} D_{a0} \equiv \sum_{a \in \mathbb{Z}^+(p)} \tilde{t}^{-a} \widetilde{D}_{a0} \,\mathrm{mod}(\sigma - \mathrm{id})\left(\mathcal{M}_k^{(1)} \otimes \mathcal{K}\right) + \mathcal{M}_k^{(1)} \otimes O_{\mathcal{K}}.$$

c) *Action of analytical automorphisms.* Consider the group $\mathrm{Aut}^1 \mathcal{K}$ of "analytical" automorphisms of the field $\mathcal{K}$, i.e. the group of automorphisms ψ of $\mathcal{K}$ such that $\psi|_k = \mathrm{id}$. Conjugation by any lifting of ψ to $\mathrm{Aut}\, \mathcal{K}_{\mathrm{sep}}$ induces the k-linear automorphism $m \mapsto \psi * m$ of $\mathcal{M}_k^{(1)}$. In terms of the special basis $\mathcal{D}^{(1)}(\tilde{t})$ this automorphism can be computed via the following formal congruence in $\mathcal{M}_k^{(1)} \otimes_k \mathcal{K}$

$$\sum_{a \in \mathbb{Z}^+(p)} \psi^{-1}(\tilde{t})^{-a} \widetilde{D}_{a0} \equiv \sum_{a \in \mathbb{Z}^+(p)} \tilde{t}^{-a}(\psi * \widetilde{D}_{a0}) \operatorname{mod}(\sigma - \mathrm{id}) \left(\mathcal{M}_k^{(1)} \otimes \mathcal{K}\right) + \mathcal{M}_k^{(1)} \otimes O_{\mathcal{K}}.$$

d) *Computaion of elements* $\tau_0 * m$. Let $P = P(X) \in W[[X]]$ be such that $P(\pi) \equiv \zeta_M \operatorname{mod} p$. Set $P_M = P^{p^M}$ and consider $\tau_P \in \operatorname{Aut}^1 \mathcal{K}$ given by the correspondence $t \mapsto tP_M(t)$. Then for any $m \in \mathcal{M}_k^{(1)}$, we have $\tau_P * m \equiv \tau_0 * m \operatorname{mod} \mathcal{M}_k^{(w_0)}$, where $w_0 = ep^M$ (we note that $v_0 > w_0 > v_0/p$).

1.4. Consider the group isomorphism G_1 from n.1.2. It can be given by a group isomorphism $G' : \mathcal{G} \longrightarrow \mathcal{G}'$ such that for any $v \in [1, v_0]$, we have $G'(\mathcal{G}^{(v)}) = \mathcal{G}'^{(v)}$. Denote by g'_k the k-linear morphism $\mathcal{M}_k^{(1)} \longrightarrow \mathcal{M}'^{(1)}_k$ induced by G'. Then for any $m \in \mathcal{M}_k^{(1)}$, we have

$$g_k(\tau_0 * m) \equiv \tau'_0 * g_k(m) \operatorname{mod} \mathcal{M}_k^{(v_0)}. \tag{2}$$

Take the uniformiser t' of $\mathcal{K}'$ from n.1.2 and consider the special basis $\mathcal{D}^{(1)}(t') = \{D'_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \operatorname{mod} N_0\}$ of $\mathcal{M}'^{(1)}_k$. For all $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z} \operatorname{mod} N_0$, set $C_{an} = g_k^{-1}(D'_{an})$. These elements create a basis of $\mathcal{M}_k^{(1)}$ and this basis can be approximated by some uniquely determined special basis. More precisely, there exist a uniformiser $\tilde{t}$ of $\mathcal{K}$ and $n_0 \in \mathbb{Z} \operatorname{mod} N_0$ such that if $\mathcal{D}^{(1)}(\tilde{t}) = \{\widetilde{D}_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z} \operatorname{mod} N_0\}$, then for any $a \in \mathbb{Z}^+(p)$,

$$\sigma^{n_0} C_{a0} = \sum_{b,m} \alpha_{abm} \widetilde{D}_{bm},$$

where the sum is taken for all $b \in \mathbb{Z}^+(p)$ such that $b \geqslant \min\{a, v_0\}$ and all $m \in \mathbb{Z} \operatorname{mod} N_0$, and all coefficients $\alpha_{abm} \in k$ satisfy the properties $\alpha_{110} = 1$, $\alpha_{1b0} = 0$ for all $b > 1$, and $\alpha_{2b0} = 0$ for $b \equiv -1 \operatorname{mod} p$ (these properties of coefficients α_{abm} provide us with uniqiness of this special basis).

Consider the field isomorphism $h : \mathcal{K} \longrightarrow \mathcal{K}'$ uniquely given by conditions $h(\tilde{t}) = t'$ and $h|_k = \sigma^{-n_0}$. Then h induces the isomorphism H of the Galois groups $\mathcal{G}$ and $\mathcal{G}'$. It induces also 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 $n \in \mathbb{Z} \operatorname{mod} N_0$.

Introduce the automorphism $F = H \circ G'^{-1}$ of the group $\mathcal{G}$. Clearly, F respects the segment $\{\mathcal{G}^{(v)}\}_{1 \leqslant v \leqslant v_0}$ of the ramification filtration. Denote by f_k the k-linear automorphism of $\mathcal{M}_k^{(1)}$ induced by F, and set $f_k(\widetilde{D}_{an}) = \sigma^{n_0} C_{an} := \widetilde{C}_{an}$. The Main Lemma from [Ab] shows that f_k must have very special form modulo $\mathcal{M}_k^{(\tilde{v}_0)}$, where $\tilde{v}_0 = v_0/p$. More precisely, for $c \in \mathbb{Z}^+(p)$ and $m \in \mathbb{N}$, there exist $\gamma_{c,-m} \in k$ such that for all $a \in \mathbb{Z}^+(p)$,

$$\widetilde{D}_{a0} \equiv \widetilde{C}_{a0} + \sum_{c,-m} \gamma_{c,-m} \widetilde{C}_{ap^m+c,-m} \operatorname{mod} \mathcal{M}_k^{(\tilde{v}_0)}. \tag{3}$$

1.5. The above relation (3) together with the formalism of Artin-Schreier theory from n.1.3 allow us to relate k-linear automorphisms $m \mapsto \tau_o * m$ of $\mathcal{M}_k^{(1)} \operatorname{mod} \mathcal{M}_k^{(\tilde{v}_0)}$ and $m \mapsto \tau_0' * m$ of $\mathcal{M}_k'^{(1)} \operatorname{mod} \mathcal{M}_k'^{(\tilde{v}_0)}$.

Namely, we can apply the properties 1.3 c) and d) to express the map $m \mapsto \tau_0 * m$ in terms of the special basis $\mathcal{D}^{(1)}(\tilde{t})$. In order to express the map $m \mapsto \tau_0' * m$ in terms of the special basis $\mathcal{D}'^{(1)}(t')$, introduce a power series $P' = P'(X) \in W[[X]]$ such that $P'(\pi') = \zeta_M' \operatorname{mod} p$, set $P_M' = P'^{p^M}$ and consider $\tau_{P'} \in \operatorname{Aut}^1 \mathcal{K}'$ given by the correspondence $t' \mapsto t' P_M'(t')$. Then we use $\tau_{P'}$ to describe explicitly the k-linear morphism $m \mapsto \tau_0' * m$, where $m \in \mathcal{M}_k'^{(1)} \operatorname{mod} \mathcal{M}_k'^{(\tilde{v}_0)}$, in terms of the special basis $\mathcal{D}^{(1)}(t')$. These formulae are transformed to the action of τ_0 in terms of elements $\widetilde{C}_{an}$ by the relation (2) of n.1.4. Finally, the relation (3) provides us with the following clue property.

If $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and

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

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

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

1.6. For $m \in \mathbb{Z} \operatorname{mod} p^M$, denote by $\mathcal{N}_m$ the k-submodules of $t^{-(\tilde{v}_0 - 1)} O_{\mathcal{K}} \operatorname{mod} O_{\mathcal{K}}$ generated by elements of the set $\{t^{-a} \mid a \in \mathbb{N} \cap [1, \tilde{v}_0), a \operatorname{mod} p^M = m\}$. Clearly, these modules are τ_P-invariant and we have the following τ_P-invariant decomposition

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

For $m \in \mathbb{Z} \operatorname{mod} p^M$, denote by pr_m the projection from $t^{-(\tilde{v}_0 - 1)} O_{\mathcal{K}} \operatorname{mod} O_{\mathcal{K}}$ to $\mathcal{N}_m$.

For $m \in \mathbb{Z} \operatorname{mod} p^M$ and $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ denote by $b(a,m)$ the minimal non-negative integer such that

$$\operatorname{pr}_m(\tilde{t}^{-a}\varepsilon_a) \in t^{-b(a,m)} O_{\mathcal{K}} \operatorname{mod} O_{\mathcal{K}}.$$

We note that if $b(a,m) \neq 0$, then $b(a,m) \operatorname{mod} p^M = m$, and if $m = a \operatorname{mod} p^M$ then $b(a,m) = a$.

If $m \not\equiv 0 \operatorname{mod} p^M$, then the formula (4) of n.1.5 implies that

$$\tau_P^{-1}(\operatorname{pr}_m(\tilde{t}^{-a}\varepsilon_a) \operatorname{mod} O_{\mathcal{K}}) = \operatorname{pr}_m(\tilde{t}^{-a}\varepsilon_a)(\sigma_*^{n_0} P_M')(\tilde{t})^a \operatorname{mod} O_{\mathcal{K}}.$$

But τ_P^{-1} acts by multiplication by $P_M(t)^m$ on $\mathcal{N}_m$, therefore,

$$(\sigma_*^{n_0} P_M')(\tilde{t})^a \equiv P_M(t)^m \operatorname{mod} t^{b(a,m)}$$

for all $m \in \mathbb{Z} \operatorname{mod} p^M$ such that $m \not\equiv 0 \operatorname{mod} p^M$ and all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$.

If we take $a = \tilde{v}_0 - 1$ and $m = a \operatorname{mod} p^M = -1 \operatorname{mod} p^M$ (we use that $M \geqslant 2$ and therefore, $\tilde{v}_0 \equiv 0 \operatorname{mod} p^M$), then the above congruence gives

$$(\sigma_*^{n_0} P_M')(\tilde{t}) \equiv P_M(t) \operatorname{mod} t^{\tilde{v}_0 - 1}, \tag{5}$$

and as in [Ab, n.5] we obtain

$$(6) \qquad (\sigma_*^{n_0}P')(\tilde{t}) \equiv P(t) \bmod t^{e/(p-1)}.$$

Now we note that the $\mathbb{Z}_p[\zeta_M]$-algebra $O_K \bmod p^{1/(p-1)}$ is isomorphic to the algebra $O_{\mathcal{K}} \bmod t^{e/(p-1)}$, with action of ζ_M induced by analytical automorphism of $\mathcal{K}$ such that $t \mapsto tP(t)$. Analogously, the $\mathbb{Z}_p[\zeta_M]$-algebra $O_{K'} \bmod p^{1/(p-1)}$ is isomorphic to the algebra $O_{\mathcal{K}'} \bmod t'^{e/(p-1)}$ with action of ζ'_M given by analytical automorphism of $\mathcal{K}'$ such that $t' \mapsto t'P'(t')$. Now the relation (6) implies that the fields isomorphism $h : \mathcal{K} \longrightarrow \mathcal{K}'$ from n.1.4 induces ϕ_M-linear automorphism of $\mathbb{Z}_p[\zeta_M]$-algebras $O_{\mathcal{K}} \bmod t^{e/(p-1)}$ and $O_{\mathcal{K}'} \bmod t'^{e/(p-1)}$, where $\phi_M(\zeta_M) = \zeta'_M$.

This also implies that the statement of our proposition is equivalent to the congruence

$$\widetilde{D}_{a0} \equiv \widetilde{C}_{a0} \bmod \mathcal{M}_k^{(p^M+1)},$$

for all $a \in \mathbb{Z}^+(p) \cap [1, p^M + 1)$.

1.7. The congruence (5) of n.1.6 implies that for all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and all $m \in \mathbb{Z} \bmod p^M$ such that $m \neq 0 \bmod p^M$, we have

$$P_M(t)^a = P_M(t)^m \bmod t^{b(a,m)}.$$

Because $P_M(t) = 1 + At^{e/(p-1)} + \dots$ with $A \neq 0$ and $m \equiv b(a,m) \bmod p^M$ if $b(a,m) \neq 0$, this gives for any $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and any $m \in \mathbb{Z} \bmod p^M$ such that $m \neq 0 \bmod p^M$, the inequality

$$b(a,m) \leqslant ep^{s+1}/(p-1),$$

where $s = v_p(a - b(a,m))$. In particular,

$$(7) \qquad \mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a) \in t^{-ep/(p-1)}O_{\mathcal{K}} \bmod O_{\mathcal{K}},$$

if $m \not\equiv a \bmod p$, but $m \neq 0 \bmod p^M$.

1.8. Consider a presentation of $\tilde{t}$ in the form

$$\tilde{t} = \alpha t(1 + Q(t) + \beta t^r + \dots) \bmod t^{\tilde{v}_0}O_{\mathcal{K}},$$

where $\alpha, \beta \in k^*$, $Q \in Xk[X]$ is such that $\deg Q < r$ and $r \in \mathbb{Z}^+(p)$.

Lemma. *In the above notation we have*

$$r \geqslant \tilde{v}_0 - 1 - ep/(p-1).$$

Corollary. *For all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and $m \in \mathbb{Z} \bmod p^M\mathbb{Z}$ such that $m \equiv 0 \bmod p$, we have*

$$\mathrm{pr}_m(\tilde{t}^{-a}) \in t^{-ep/(p-1)}O_{\mathcal{K}} \bmod O_{\mathcal{K}}.$$

Proof of lemma. Clearly,

$$\tilde{t}^{-\tilde{v}_0+1} = \alpha_1 t^{-\tilde{v}_0+1}(1 + Q_1(t)^p + \beta_1 t^r + \dots) \bmod O_{\mathcal{K}},$$

where $\alpha_1, \beta_1 \in k^*$, $Q_1 \in Xk[X]$, $\deg Q_1 < r$.

If $r+1 \not\equiv 0 \bmod p$, then for $m = -(r+1) \bmod p^M$, we have

$$\mathrm{pr}_m(\tilde{t}^{-\tilde{v}_0+1}) = \alpha_1\beta_1 t^{-\tilde{v}_0+1+r} + \ldots \bmod O_{\mathcal{K}}.$$

Because $m \not\equiv (\tilde{v}_0 - 1) \bmod p$, the formula (7) of n.1.7 gives

$$\mathrm{pr}_m(\tilde{t}^{-\tilde{v}_0+1}\varepsilon_{\tilde{v}_0-1}) \in t^{-ep/(p-1)}O_{\mathcal{K}} \bmod O_{\mathcal{K}}.$$

Note that $m \not\equiv 0 \bmod p$ implies that $\mathrm{pr}_m(\tilde{t}^{-\tilde{v}_0+1}) = \mathrm{pr}_m(\tilde{t}^{-\tilde{v}_0+1}\varepsilon_{\tilde{v}_0-1})$. Therefore, $-(\tilde{v}_0-1)+r \geqslant -ep/(p-1)$, i.e. the lemma is proved in the case $r+1 \not\equiv 0 \bmod p$.

If $r+1 \equiv 0 \bmod p$, then we can proceed similarly, to prove for $m = -(r+2) \bmod p^M$ that $\mathrm{pr}_m(\tilde{t}^{-\tilde{v}_0+2}) = \alpha_2\beta_2 t^{-\tilde{v}_0+2+r} + \ldots \bmod O_{\mathcal{K}}$. This gives $r \geqslant \tilde{v}_0 - 2 - ep/(p-1)$, but $r \equiv -1 \bmod p$ and $\tilde{v}_0 \equiv 0 \bmod p$ imply that $r \geqslant \tilde{v}_0 - 1 - ep/(p-1)$. The lemma is proved.

1.9. From nn.1.7 and 1.8 it follows that for all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$ and $m \in \mathbb{Z} \bmod p^M$ such that $m \not\equiv 0 \bmod p^M$ and $m \equiv 0 \bmod p$, we have

$$\mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a - \tilde{t}^{-a}) \in t^{-ep/(p-1)}O_{\mathcal{K}}.$$

For trivial reasons we have $\mathrm{pr}_m(\tilde{t}^{-a}\varepsilon_a - \tilde{t}^{-a}) = 0$, if $m \not\equiv 0 \bmod p$.

Thus, we obtained that for all $a \in \mathbb{Z}^+(p) \cap [1, \tilde{v}_0)$,

$$\tilde{t}^{-a} \sum_{c,m} \sigma^m(\gamma_{c,-m})\tilde{t}^c \in t^{-ep/(p-1)}O_{\mathcal{K}} + \sigma^M\mathcal{K},$$

where the sum is taken for $1 \leqslant m < M$ and $c \in \mathbb{Z}^+(p)$ such that $v_p(a-c) = m$.

This gives the following property of elements $\gamma_{c,-m}$

if $1 \leqslant m < M$ *and there exists* $a_1 \in (c, \tilde{v}_0 - ep/(p-1))$ *such that* $v_p(a_1 - c) = m$, *then* $\gamma_{c,-m} = 0$.

Assume that $c \in \mathbb{Z}^+(p)$ and $1 \leqslant m < M$. If there exists $a \in \mathbb{Z}^+(p)$ such that $ap^m + c \leqslant a^*$, where $a^* = \min\{p^M+1, \tilde{v}_0 - ep/(p-1)\}$, then we can use $a_1 = ap^m + c$ to deduce that $\gamma_{c,-m} = 0$ from the above property of these elements. Therefore, $\widetilde{D}_{a0} = \widetilde{C}_{a0}$ for all $a \in \mathbb{Z}^+(p) \cap [1, a^*)$. It remains only to note that for $M \geqslant 2$,

$$\tilde{v}_0 - ep/(p-1) = ep(p^{M-1}-1)/(p-1) \geqslant e_{\mathbb{Q}_p(\zeta_M)}p(p^{M-1}-1)/(p-1) > p^M + 1,$$

i.e. $a^* = p^M + 1$. The proposition is proved.

2. Proof of the theorem.

2.1. Let $\widetilde{E} \in \mathcal{F}_{\mathbb{Q}_p}$ be a Galois extension of the field E. Then $\Gamma_{\widetilde{E}} \subset \Gamma_E$ and $F(\Gamma_{\widetilde{E}}) = \Gamma_{\widetilde{E}'} \subset \Gamma_{E'}$, where $\widetilde{E}'$ is a finite Galois extension of E'. Then F induces the group isomorphism $F_{\widetilde{E}} : \Gamma_{\widetilde{E}/E} \longrightarrow \Gamma_{\widetilde{E}'/E'}$.

Because the centraliser of the subgroup Γ_E in $\Gamma_{\mathbb{Q}_p}$ is trivial, our theorem is implied by the following proposition.

Proposition. *There exists a field isomorphism* $f_{\widetilde{E}} : \widetilde{E} \longrightarrow \widetilde{E}'$ *such that* $f_{\widetilde{E}}(E) = E'$ *and for any* $g \in \Gamma_{\widetilde{E}/E}$ *one has* $F_{\widetilde{E}}(g) = f_{\widetilde{E}}^{-1} g f_{\widetilde{E}}$.

Proof of proposition. Without loss of generality we can assume in the proof (cf. nn.2.2-2.6 below) that $\widetilde{E}$ is a finite Galois extension of $\mathbb{Q}_p$.

2.2. For $s \in \mathbb{Z}_{\geqslant 0}$ set $\widetilde{E}_s = \widetilde{E}(\zeta_s)$, where ζ_s is as usually a primitive root of unity of degree p^s. Denote by $\widetilde{E}_\infty$ the union of all $\widetilde{E}_s$. Then $\widetilde{E}_\infty$ is an infinite strict arithmetical profinite extension of $\mathbb{Q}_p$. The following two properties a) and b) of such extensions are well-known, cf. [Wi].

a) For $x \geqslant 0$, there exists a limit $\varphi_\infty(x) = \lim\limits_{s\to\infty} \varphi_{\widetilde{E}_s/\mathbb{Q}_p}(x)$, where for any $s \in \mathbb{Z}_{\geqslant 0}$, $\varphi_{\widetilde{E}_s/\mathbb{Q}_p}$ is Herbrand's function of the extension $\widetilde{E}_s/\mathbb{Q}_p$. For all indices s, there exist $C_s \in \mathbb{R}$ such that $\lim\limits_{s\to\infty} C_s = +\infty$ and for any $x \in [0, C_s]$ and $u \geqslant s$, one has $\varphi_\infty(x) = \varphi_{\widetilde{E}_u/\mathbb{Q}_p}(x)$.

We apply this property to prove the following statement.

Lemma. *There exists an index* s_0 *and a number* $\tilde{x}_0 > 0$ *such that for any* $s \geqslant s_0$ *and any* $x > \tilde{x}_0$*, the ramification subgroup (in lower numbering)* $\Gamma_{\widetilde{E}_s/\mathbb{Q}_p, x}$ *acts trivially on* $\widetilde{E}$.

Proof. Let $\tilde{v}_0 = v(\tilde{E}/\mathbb{Q}_p)$ be the maximal upper ramification number for the extension $\tilde{E}/\mathbb{Q}_p$ (recall that $\tilde{v}_0$ is the maximal number such that $\Gamma_{\mathbb{Q}_p}^{(\tilde{v}_0)}$ acts nontrivially on $\widetilde{E}$). Let $\tilde{x}_0 \geqslant 0$ be such that $\tilde{v}_0 = \varphi_\infty(\tilde{x}_0)$ and let an index s_0 be such that $C_s > \tilde{x}_0$ for all $s \geqslant s_0$. If $s \geqslant s_0$ and $x > \tilde{x}_0$, then $x_s := \min\{x, C_s\} > \tilde{x}_0$ and

$$\Gamma_{\tilde{E}_s/\mathbb{Q}_p, x} = \Gamma_{\tilde{E}_s/\mathbb{Q}_p}^{(\varphi_s(x))} \subset \Gamma_{\tilde{E}_s/\mathbb{Q}_p}^{(\varphi_s(x_s))} = \Gamma_{\tilde{E}_s/\mathbb{Q}_p}^{(\varphi_\infty(x_s))}$$

acts trivially on $\tilde{E}$ because $\varphi_\infty(x_s) > \varphi_\infty(\tilde{x}_0) = \tilde{v}_0$. The lemma is proved.

b) Let $\widetilde{\mathcal{E}} = \mathcal{X}(\widetilde{E}_\infty)$ and $\mathcal{K}_0 = \mathcal{X}(\bigcup\limits_{s\geqslant 0} \mathbb{Q}_p(\zeta_s))$, where $\mathcal{X}$ is the field-of-norms functor. Then $\mathcal{K}_0$ is a complete discrete valuation field, $\mathcal{E}$ is its finite Galois extension, and there exists s_1 such that for all $s \geqslant s_1$, Herbrand's functions coincide $\varphi_{\widetilde{E}_s/\mathbb{Q}_p(\zeta_s)} = \varphi_{\widetilde{\mathcal{E}}/\mathcal{K}_0}$.

In particular, if $s \geqslant s_1$ then $[\widetilde{\mathcal{E}} : \mathcal{K}_0] = [\widetilde{E}_s : \mathbb{Q}_p(\zeta_s)]$, the ramification indices of all extensions $\widetilde{E}_s/\mathbb{Q}_p(\zeta_s)$ are equal to the ramification index $\tilde{e}$ of the extension $\widetilde{\mathcal{E}}/\mathcal{K}_0$, and we have the equality of the largest upper ramification numbers $v(\widetilde{\mathcal{E}}/\mathcal{K}_0) = v(\widetilde{E}_s/\mathbb{Q}_p(\zeta_s))$.

2.3. For any index $s \geqslant s_1$, choose an unramified extension L_s of E_s such that if k_s is the residue field of L_s then $[k_s : \mathbb{F}_p] \geqslant 2(s+1) + \log_p \tilde{e}$. We note that the field L_s satisfies the assumptions for the field K from n.1.1 with $M = s$. Indeed, $\log_p(p^2 v_{L_s}) = 2(s+1) + \log_p \tilde{e}$, because $v_{L_s} = e_{L_s} p^{s+1}/(p-1)$ and $e_{L_s} = \tilde{e} p^{s-1}(p-1)$.

If $F(\Gamma_{L_s}) = \Gamma_{L'_s}$, then L'_s is a finite Galois extension of E', F induces the group isomorphisms

$$F_{L_s} : \Gamma_{L_s/E} \longrightarrow \Gamma_{L'_s/E'},$$

$$F_s : \Gamma_{L_s} \longrightarrow \Gamma_{L'_s},$$

and these isomorphisms are compatible with ramification filtrations.

2.4. By the above construction, the fields L_s are unramified over $\widetilde{E}_s$, therefore, $v(L_s/\mathbb{Q}_p(\zeta_s)) = v(E_s/\mathbb{Q}_p(\zeta_s)) = v(\widetilde{\mathcal{E}}/\mathcal{K}_0) = \tilde{v}$ do not depend on the index $s \geqslant s_1$. Let an index $s_2 \geqslant s_1$ be such that $p^{s_2-1} - 1 > \tilde{v}$. By the main result of [Ab], cf. n.1.1, we have for all $s \geqslant s_2$, a ϕ_s-linear isomorphism of $\mathbb{Z}_p[\zeta_s]$-algebras

$$\tilde{\phi}_s : O_{L_s} \operatorname{mod} p^{1/(p-1)} \longrightarrow O_{L'_s} \operatorname{mod} p^{1/(p-1)},$$

where ϕ_s is some automorphism of the field $\mathbb{Q}_p(\zeta_s)$.

Because $p^{s-1} - 1 > \tilde{v}$, this implies for all $s \geqslant s_2$, the existence of field isomorphisms $f_s : L_s \longrightarrow L'_s$ such that f_s and $\tilde{\phi}_s$ induce the same map

$$O_{L_s} \operatorname{mod} p^{1/(p-1)-\varepsilon_s} \longrightarrow O_{L'_s} \operatorname{mod} p^{1/(p-1)-\varepsilon_s},$$

where all $\varepsilon_s > 0$ and $\lim\limits_{s\to\infty} \varepsilon_s = 0$.

Indeed, let $m_{\mathbb{Q}_p(\zeta_s)}$ and m_{L_s} be maximal ideals in $\mathbb{Z}_p[\zeta_s]$ and O_{L_s} respectively. Then $(p^{1/(p-1)}) = m_{\mathbb{Q}_p(\zeta_s)}^{p^{s-1}}$. Now we obtain from [De, rem.A.6.3] the existence (and even the uniqiuness) of a fields isomorphism f_s, such that its restriction to O_{L_s} and $\tilde{\phi}_s$ coincide when taken modulo $m_{L_s}^{\psi_{L_s/\mathbb{Q}_p(\zeta_s)}(p^{s-1}-1)+1}$, where $\psi_{L_s/\mathbb{Q}_p(\zeta_s)}$ is the inverse function for Herbrand's function of the extension $L_s/\mathbb{Q}_p(\zeta_s)$.

Our property follows now easily because for $s \geqslant s_2$, we have $e_{L_s} = \tilde{e}e_{\mathbb{Q}_p(\zeta_s)} = \tilde{e}p^{s-1}(p-1)$, $\psi_{L_s/\mathbb{Q}_p(\zeta_s)} = \psi_{\widetilde{\mathcal{E}}/\mathcal{K}_0}$ does not depend on s, and for some $C > 0$ one has for all x the following inequalities

$$\tilde{e}x - C < \psi_{\widetilde{\mathcal{E}}/\mathcal{K}_0}(x) < \tilde{e}x.$$

2.5. Let $s \geqslant s_2$ and choose $\tau_s \in \Gamma_{\mathbb{Q}_p}$ such that $\tau_s|_{L_s} = f_s$. Set $\widetilde{E}'' = \tau_s^{-1}\widetilde{E}'$ and $E'' = \tau_s^{-1}E'$, and consider the group isomorphism $G_s = F \circ \tau_s^* : \Gamma_E \longrightarrow \Gamma_{E''}$.

Take an arbitrary $\tau \in \Gamma_E$, then $G_s(\tau) \in \Gamma_{E''}$, and set

$$\gamma_s(\tau) = \tau^{-1}G_s(\tau) \in \Gamma_{\mathbb{Q}_p}.$$

Because L_s is a Galois extension of $\mathbb{Q}_p$, elements of the group $\Gamma_{\mathbb{Q}_p}$ act by conjugation on the maximal abelian quotient $\Gamma_{L_s}^{\mathrm{ab}}$ of Γ_{L_s}. By Proposition n.1, the action of $\gamma_s(\tau)$ on $\Gamma_{L_s}^{\mathrm{ab}}$ induces the identity map on its subquotient $\Gamma_{L_s}^{\mathrm{ab}(1)} \operatorname{mod} \left(\Gamma_{L_s}^{\mathrm{ab}}\right)^p \Gamma_{L_s}^{\mathrm{ab}(p^s+1)}$ (of course, we assume that $s_2 \geqslant 2$). Indeed, by Proposition n.1 G_s induces the identity map on this subquotient. But G_s transforms the conjugation by τ to the conjugation by $G_s(\tau)$ therefore, these conjugations coincide on our subquotient.

Now we apply local class field theory to conclude that the automorphism $\gamma_s(\tau)$ of the field L_s acts trivially on $U_{L_s}^{(1)} \operatorname{mod} U_{L_s}^p U_{L_s}^{(p^s+1)}$.

Let π be a uniformiser of L_s, then we have

$$\gamma_s(\tau)(1+\pi) = (1+\pi)(1+\alpha_1)^p \operatorname{mod} m_{L_s}^{p^s+1},$$

$$\gamma_s(\tau)(1+\pi^2) = (1+\pi^2)(1+\alpha_2)^p \operatorname{mod} m_{L_s}^{p^s+1},$$

for some $\alpha_1, \alpha_2 \in m_{L_s}$. Assume that $\beta = \gamma_s(\tau)(\pi) - \pi \notin m_{L_s}^{p^s}$. Then the above two congruences give the contradiction:

$$\alpha_1^p \equiv \beta \operatorname{mod} \beta m_{L_s}, \quad \alpha_2^p \equiv \pi\beta \operatorname{mod} \beta m_{L_s}^2.$$

Therefore, $\beta \in m_{L_s}^{p^s}$, i.e. the image $\bar{\gamma}_s(\tau)$ of $\gamma_s(\tau)$ in the Galois group $\Gamma_{L_s/\mathbb{Q}_p}$ belongs to its ramification subgroup (in lower numbering) $\Gamma_{L_s/\mathbb{Q}_p, p^s-1}$.

So, we proved the following statement.

Lemma. *There exists an index $s_2 \geqslant 2$ such that for all $s \geqslant s_2$ and $\tau \in \Gamma_E$, one has $\bar{\gamma}_s(\tau) \in \Gamma_{L_s/\mathbb{Q}_p, p^s-1}$.*

2.6. Choose an index s such that $s \geqslant \max\{s_2, s_0\}$ and $p^s - 1 > \tilde{x}_0$, cf. Lemma n.2.2. Then any element of the ramification subgroup $\Gamma_{\widetilde{E}_s/\mathbb{Q}_p, p^s-1}$ acts trivially on $\widetilde{E}$, i.e. $\Gamma_{\widetilde{E}_s/\mathbb{Q}_p, p^s-1} \subset \Gamma_{\widetilde{E}_s/\widetilde{E}}$. But the extension $L_s/\widetilde{E}_s$ is unramified, therefore, the image of $\gamma_s(\tau)$ in $\Gamma_{\widetilde{E}_s/\mathbb{Q}_p}$ belongs to the ramification subgroup $\Gamma_{\widetilde{E}_s/\mathbb{Q}_p, p^s-1}$. This gives finally that $\gamma_s(\tau) \in \Gamma_{\widetilde{E}}$ or

$$G_s(\tau) \equiv \tau \bmod \Gamma_{\widetilde{E}} \tag{8}$$

for any $\tau \in \Gamma_E$.

Therefore, in notation of n.2.5 we have $E'' = E$ and $\widetilde{E}'' = \widetilde{E}$, because the above congruence (8) implies the following implications:

$$\tau \in \Gamma_E \ \Rightarrow \ G_s(\tau) \in \Gamma_E \ \Rightarrow \ \tau \in \Gamma_{E''},$$

$$\tau \in \Gamma_{\widetilde{E}} \ \Rightarrow \ G_s(\tau) \in \Gamma_{\widetilde{E}} \ \Rightarrow \ \tau \in \Gamma_{\widetilde{E}''}.$$

From the congruence (8) it follows also that the group morphism $G_s = F \circ \tau_s^*$ induces the identity automorphism of the Galois group $\Gamma_{\widetilde{E}/E}$. Therefore, the group morphism

$$F_{\widetilde{E}} : \Gamma_{\widetilde{E}/E} \longrightarrow \Gamma_{\widetilde{E}'/E'}$$

comes from the conjugation by the $\tau_s \in \Gamma_{\mathbb{Q}_p}$ chosen in n.2.5. So, the statement of our proposition holds for $f_{\widetilde{E}} = \tau_s|_{\widetilde{E}}$.

The proposition and the theorem are completely proved.

References

[Ab] V.A. Abrashkin, *A strong property of ramification filtration*, Preprint MPI (Bonn) **38** (1998).

[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.

[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