JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Victor ABRASHKIN

Modified proof of a local analogue of the Grothendieck conjecture

Tome 22, n° 1 (2010), p. 1-50.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_1_0>

Journal de Théorie des Nombres de Bordeaux **22** (2010), 1-50

Modified proof of a local analogue of the Grothendieck conjecture

par Victor ABRASHKIN

Résumé. L'analogue local de la conjecture de Grothendieck peut être formulé comme une équivalence entre la catégorie des corps K complets pour une valuation discrete à corps résiduel fini de caractéristique $p \neq 0$ et la catégorie des groupes de Galois absolus des corps K munis de la filtration de ramification. Le cas des corps de caractéristique 0 a été étudié par Mochizuki il y a quelques années. Ensuite, l'auteur de cet article a établi, par une méthode différente l'analogue de la conjecture de Grothendieck dans le cas $p > 2$ (mais K de caractéristique quelconque). Nous proposons ici une modification de cette approche qui inclut le cas $p = 2$ dans la preuve, contient des simplifications considérables et remplace le groupe de Galois par son pro-p-quotient maximal. Une attention particulière est accordée au procédé de la reconstruction de l'isomorphisme de corps à partir d'un isomorphisme de groupe de Galois compatible avec les filtrations de ramification correspondantes.

Abstract. A local analogue of the Grothendieck Conjecture is an equivalence between the category of complete discrete valuation fields K with finite residue fields of characteristic $p \neq 0$ and the category of absolute Galois groups of fields K together with their ramification filtrations. The case of characteristic 0 fields K was studied by Mochizuki several years ago. Then the author of this paper proved it by a different method in the case $p > 2$ (but with no restrictions on the characteristic of K). In this paper we suggest a modified approach: it covers the case $p = 2$, contains considerable technical simplifications and replaces the Galois group of K by its maximal pro-p-quotient. Special attention is paid to the procedure of recovering field isomorphisms coming from isomorphisms of Galois groups, which are compatible with the corresponding ramification filtrations.

Introduction

Throughout this paper p is a prime number. If E is a complete discrete valuation field then we shall assume that its residue field has characteristic

Manuscrit reçu le 9 mars 2007, révisé le 13 juillet 2009.

p. We will consider E to be a subfield of a fixed separable closure E_{sep}. Define $\Gamma_E = \mathrm{Gal}(E_{\mathrm{sep}}/E)$. We denote by $E(p)$ the maximal p-extension of E in E_{sep} and we let $\Gamma_E(p) = \mathrm{Gal}(E(p)/E)$.

Assume that E and E' are complete discrete valuation fields with finite residue fields and there is a continuous field isomorphism $\mu : E \longrightarrow E'$. Then μ can be extended to a field isomorphism $\bar{\mu} : E(p) \longrightarrow E'(p)$. With the conventions about compositions of morphisms which are described at the end of this introduction, the correspondence $\tau \mapsto \bar{\mu}^{-1}\tau\bar{\mu}$ defines a continuous group isomorphism $\bar{\mu}^* : \Gamma_E(p) \longrightarrow \Gamma_{E'}(p)$ such that for any $v \geqslant 0$, $\bar{\mu}^*(\Gamma_E(p)^{(v)}) = \Gamma_{E'}(p)^{(v)}$. Here $\Gamma_E(p)^{(v)}$ is the ramification subgroup of $\Gamma_E(p)$ in the upper numbering.

The principal result of this paper is the following theorem.

Theorem A. *Suppose E and E' are complete discrete valuation fields with finite residue fields and there is a continuous group isomorphism $g : \Gamma_E(p) \longrightarrow \Gamma_{E'}(p)$ such that for all $v \geqslant 0$, $g(\Gamma_E(p)^{(v)}) = \Gamma_{E'}(p)^{(v)}$. Then there is a continuous field isomorphism $\bar{\mu} : E(p) \longrightarrow E'(p)$ such that $\bar{\mu}(E) = E'$ and $g = \bar{\mu}^*$.*

This theorem implies easily a corresponding statement, where the maximal p-extensions $E(p)$ and $E'(p)$ and their Galois groups $\Gamma_E(p)$ and $\Gamma_{E'}(p)$ are replaced, respectively, by the separable closures E_{sep} and E'_{sep} and the Galois groups Γ_E and $\Gamma_{E'}$. Such a statement is known as a local analogue of the Grothendieck Conjecture. Mochizuki [7] proved this local analogue for local fields of characteristic 0. His method is based on an elegant application of Hodge-Tate theory. Under the restriction $p > 2$ the case of local fields of arbitrary characteristic was proved by another method by the author [3]. This proof is based on an explicit description of the ramification subgroups $\Gamma_K(p)^{(v)}$ modulo the subgroup $C_3(\Gamma_K(p))$ of commutators of order $\geqslant 3$ in $\Gamma_K(p)$, where $K = k((t))$, and k is a finite field of characteristic $p > 2$. The restriction $p \neq 2$ appears because the proof uses the equivalence of the category of p-groups and of Lie $\mathbb{Z}_p$-algebras of nilpotent class 2, which holds only under the assumption $p > 2$.

The statement of Theorem A is free from the restriction $p \neq 2$. Its proof follows mainly the strategy from [3] but there are several essential changes.

Firstly, instead of working with the ramification subgroups $\Gamma_K(p)^{(v)}$, $v \geqslant 0$, we fix the simplest possible embedding of $\Gamma_K(p)$ into its Magnus's algebra $\mathcal{A}$ and study the induced fitration by the ideals $\mathcal{A}^{(v)}$, $v \geqslant 0$, of $\mathcal{A}$. As a result, we obtain an explicit description of the ideals $\mathcal{A}^{(v)} \bmod \mathcal{J}^3$, where $\mathcal{J}$ is the augmentation ideal in $\mathcal{A}$. This corresponds to the description of the groups $\Gamma_K(p)^{(v)} \bmod C_3(\Gamma_K(p))$ in [1] but it is easier to obtain and it works for all prime numbers p including $p = 2$.

Secondly, any continuous group automorphism of $\Gamma_K(p)$ which is compatible with the ramification filtration induces a continuous algebra automorphism f of $\mathcal{A}$ such that for any $v \geqslant 0$, $f(\mathcal{A}^{(v)}) = \mathcal{A}^{(v)}$. Similarly to [3], the conditions $f(\mathcal{A}^{(v)}) \operatorname{mod} \mathcal{J}^3 = \mathcal{A}^{(v)} \operatorname{mod} \mathcal{J}^3$ imply non-trivial properties of the restriction of the original automorphism of $\Gamma_K(p)$ to the inertia subgroup $I_K(p)^{\mathrm{ab}}$ of the Galois group of the maximal abelian extension of K. These properties are studied in detail in this paper. This allows us to give a more detailed and effective version of the final stage of the proof of the local analogue of the Grothendieck Conjecture even in the case $p \neq 2$. In particular, this clarifies why it holds with the absolute Galois groups replaced by the Galois groups of maximal p-extensions.

The methods of this paper can be helpful for understanding the relations between fields and their Galois groups in the context of the global Grothendieck Conjecture. For example, suppose F is an algebraic number field, $\bar{F}$ is its algebraic closure, $\Gamma_F = \mathrm{Gal}(\bar{F}/F)$, $\wp$ is a prime divisor in F, $\bar{\wp}$ is its extension to $\bar{F}$ and $F_\wp$, $\bar{F}_{\bar{\wp}}$ are the corresponding completions of F and $\bar{F}$, respectively. Then $\Gamma_{F,\bar{\wp}} = \mathrm{Gal}(\bar{F}_{\bar{\wp}}/F_\wp) \subset \Gamma_F$ is the decomposition group of $\bar{\wp}$. Suppose F is Galois over $\mathbb{Q}$ and $g_\wp : \Gamma_{F,\bar{\wp}} \longrightarrow \Gamma_{F,\bar{\wp}}$ is a continuous group automorphism which is compatible with the ramification filtration on $\Gamma_{F,\bar{\wp}}$. By the local analogue of the Grothendieck Conjecture, $g_\wp$ is induced by a field automorphism $\bar{\mu}_\wp : \bar{F}_{\bar{\wp}} \longrightarrow \bar{F}_{\bar{\wp}}$ such that $\bar{\mu} := \bar{\mu}_{\bar{\wp}}|_{\bar{F}}$ maps $\bar{F}$ to $\bar{F}$ (because $\bar{\mu}(\mathbb{Q}) = \mathbb{Q}$), and, therefore, F to F (because F is Galois over $\mathbb{Q}$). So, $\bar{\mu}$ induces a group automorphism g of Γ_F, which extends the automorphism $g_\wp$ of $\Gamma_{F,\bar{\wp}}$, and we obtain the following criterion:

Criterion. *A group automorphism $g_\wp \in \mathrm{Aut}\Gamma_{F,\bar{\wp}}$ can be extended to a group automorphism $g \in \mathrm{Aut}\Gamma_F$ if and only if $g_\wp$ is compatible with the ramification filtration on $\Gamma_{F,\bar{\wp}}$.*

It would be interesting to understand how "global" information about the embedding of $\Gamma_{F,\wp}$ into Γ_F is reflected in "local" properties of the ramification filtration of $\Gamma_{F,\bar{\wp}}$.

Everywhere in the paper we use the following agreement about compositions of morphisms: if $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are morphisms then their composition will be denoted by fg, in other words, if $a \in A$ then $(fg)(a) = g(f(a))$. One of the reasons is that when operating on morphisms (rather than on their values in $a \in A$) the notation fg reflects much better the reality that it is the composition of the first morphism f and the second one g.

The author is very grateful to Ruth Jenni for very careful checking of the final version of this paper and pointing out various inexactitudes and misprints.

1. An analogue of the Magnus algebra for $\Gamma(p)$

In this section $K=k((t_K))$ is the local field of formal Laurent series with residue field $k=\mathbb{F}_{q_0}$, where $q_0=p^{N_0}$, $N_0\in\mathbb{N}$, and t_K is a fixed uniformiser of K (in most cases t_K will be denoted just by t). We fix a choice of a separable closure K_{sep} of K, denote by $K(p)$ the maximal p-extension of K in K_{sep} and set $\Gamma=\mathrm{Gal}(K_{\mathrm{sep}}/K)$, $\Gamma(p)=\mathrm{Gal}(K(p)/K)$.

1.1. Liftings. Notice first, that the uniformiser t_K of K can be taken as a p-basis for any finite extension L of K in K_{sep}. For $M\in\mathbb{N}$, set

$$O_M(L)=W_M(\sigma^{M-1}L)[t_{K,M}]\subset W_M(L),$$

where W_M is the functor of Witt vectors of length M, σ is the p-th power map and $t_{K,M}=[t_K]=(t_K,0,\dots,0)\in W_M(L)$ is the Teichmüller representative of t_K. Very often we shall use the simpler notation t for $t_{K,M}$ (as well as for t_K). $O_M(L)$ is a lifting of L modulo p^M or, in other words, it is a flat $W_M(\mathbb{F}_p)$-module such that $O_M(L)\bmod p=L$. This is a special case of the construction of liftings in [4].

Let $O_M(K_{\mathrm{sep}})$ be the inductive limit of all $O_M(L)$, where $L\subset K_{\mathrm{sep}}$, $[L:K]<\infty$. Then we have a natural action of Γ on $O_M(K_{\mathrm{sep}})$ and $O_M(K_{\mathrm{sep}})^\Gamma=O_M(K)=W_M(k)((t))$. We shall use again the notation σ for the natural extension of σ to $O_M(K_{\mathrm{sep}})$. Clearly, $O_M(K_{\mathrm{sep}})|_{\sigma=\mathrm{id}}=W_M(\mathbb{F}_p)$. Introduce the absolute liftings $O(K)=\varprojlim_M O_M(K)$ and $O(K_{\mathrm{sep}})=\varprojlim_M O_M(K_{\mathrm{sep}})$. Again we have $O(K_{\mathrm{sep}})^\Gamma=O(K)$ and $O(K_{\mathrm{sep}})|_{\sigma=\mathrm{id}}=W(\mathbb{F}_p)$. We can also consider the liftings $O_M(K(p))$ and $O(K(p))$ with the natural action of $\Gamma(p)$ and similar properies.

Notice that for any $j\in O(K(p))$ there is an $i\in O(K(p))$ such that $\sigma(i)-i=j$.

1.2. The algebra $\mathcal{A}$. Set $\mathbb{Z}(p)=\{a\in\mathbb{N}\mid (a,p)=1\}$ and $\mathbb{Z}^0(p)=\mathbb{Z}(p)\cup\{0\}$. Let $\mathcal{A}_k$ be the profinite associative $W(k)$-algebra with the set of pro-free generators $\{D_{an}\mid a\in\mathbb{Z}(p), n\in\mathbb{Z}\bmod N_0\}\cup\{D_0\}$.

This means that $\mathcal{A}_k=\varprojlim_{C,M}\mathcal{A}_{CMk}$, where $C,M\in\mathbb{N}$,

$$\mathcal{A}_{CMk}=W_M(k)[[\{D_{an}\mid a\leqslant C, n\in\mathbb{Z}\bmod N_0\}]]$$

and the connecting morphisms $\mathcal{A}_{C_1M_1k}\longrightarrow\mathcal{A}_{C_2M_2k}$ are defined for $C_1\geqslant C_2$, $M_1\geqslant M_2$ and induced by the correspondences $D_{an}\mapsto 0$ if $C_2<a\leqslant C_1$ and $D_{an}\mapsto D_{an}$ if $a\leqslant C_2$, and by the morphism $W_{M_1}(k)\longrightarrow W_{M_2}(k)$ of reduction modulo p^{M_2}.

Denote again by σ the extension of the automorphism σ of $W(k)$ to $\mathcal{A}_k$ via the correspondences $\sigma: D_{an}\mapsto D_{a,n+1}$, where $a\in\mathbb{Z}(p)$, $n\in\mathbb{Z}\bmod N_0$, and the correspondence $D_0\mapsto D_0$. Then $\mathcal{A}:=\mathcal{A}_k|_{\sigma=\mathrm{id}}$ is a pro-free $\mathbb{Z}_p$-algebra: if $\beta_1, \dots, \beta_{N_0}$ is a $\mathbb{Z}_p$-basis of $W(k)$ and, for $a \in \mathbb{Z}(p)$ and $1 \leqslant r \leqslant N_0$,

$$D_a^{(r)} := \sum_{n \in \mathbb{Z} \bmod N_0} \sigma^n(\beta_r) D_{an},$$

then $\{D_a^{(r)} \mid a \in \mathbb{Z}(p), 1 \leqslant r \leqslant N_0\} \cup \{D_0\}$ is a set of pro-free generators of $\mathcal{A}$. Notice also that if $\alpha_1, \dots, \alpha_{N_0} \in W(k)$ is a dual basis for $\beta_1, \dots, \beta_{N_0}$ (i.e. $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij}$, where $1 \leqslant i, j \leqslant N_0$ and Tr is the trace of the field extension $W(k) \otimes \mathbb{Q}_p$ over $\mathbb{Q}_p$) then for any $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z} \bmod N_0$, it holds

$$D_{an} = \sum_{1 \leqslant r \leqslant N_0} \sigma^n(\alpha_r) D_a^{(r)}.$$

Denote by $\mathcal{J}$, resp. $\mathcal{J}_{CM}$, the augmentation ideal in $\mathcal{A}$, resp. $\mathcal{A}_{CM}$. Set $\mathcal{A}_K := \mathcal{A} \hat{\otimes} O(K)$, $\mathcal{A}_{CMK} = \mathcal{A}_{CM} \hat{\otimes} O(K)$, $\mathcal{A}_{K(p)} = \mathcal{A} \hat{\otimes} O(K(p))$. We shall also use similar notation in other cases of extensions of scalars, e.g. $\mathcal{J}_k = \mathcal{J} \hat{\otimes} W(k)$, $\mathcal{J}_K = \mathcal{J} \hat{\otimes} O(K)$, $\mathcal{J}_{K(p)} = \mathcal{J} \hat{\otimes} O(K(p))$.

1.3. The embeddings ψ_f. Take $\alpha_0 \in W(k)$ such that $\mathrm{Tr}(\alpha_0) = 1$, where again Tr is the trace of the field extension $W(k) \otimes \mathbb{Q}_p \supset \mathbb{Q}_p$. For all $n \in \mathbb{Z} \bmod N_0$, set $D_{0n} = \sigma^n(\alpha_0) D_0$ and introduce the element

$$e = 1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} D_{a0} \in 1 + \mathcal{J}_K.$$

We shall use the same notation e for the projections of e to any of $\mathcal{A}_{CMK} \bmod \mathcal{J}^n_{CMK}$, where $C, M, n \in \mathbb{N}$.

Proposition 1.1. *There is an $f \in 1 + \mathcal{J}_{K(p)}$ such that $\sigma(f) = fe$.*

Proof. For $C, M, n \in \mathbb{N}$, set

$$S_{CMn} = \left\{ f \in 1 + \mathcal{J}_{CMK(p)} \bmod \mathcal{J}^n_{CMK(p)} \mid \sigma f = fe \bmod \mathcal{J}^n_{CMK(p)} \right\}.$$

We use induction on $n \in \mathbb{N}$ to prove that for all $C, M, n \in \mathbb{N}$, $S_{CMn} \neq \emptyset$.

Clearly, $S_{CM1} = \{1\} \neq \emptyset$.

Suppose that $S_{CMn} \neq \emptyset$ and $f \in S_{CMn}$. Then $\sigma(f) = fe \bmod \mathcal{J}^n_{CMK(p)}$. Let

$$\pi : 1 + \mathcal{J}_{CMK(p)} \bmod \mathcal{J}^{n+1}_{CMK(p)} \longrightarrow 1 + \mathcal{J}_{CMK(p)} \bmod \mathcal{J}^n_{CMK(p)}$$

be the natural projection. If $f_1 \in 1 + \mathcal{J}_{CMK(p)} \bmod \mathcal{J}^{n+1}_{CMK(p)}$ is such that $\pi(f_1) = f$ then $\sigma(f_1) = f_1 e + j \bmod \mathcal{J}^{n+1}_{CMK(p)}$, where $j \in \mathcal{J}^n_{CMK(p)}$. There is an $i \in \mathcal{J}^n_{CMK(p)}$ such that $\sigma(i) - i = j$, cf. n.1.1. Therefore,

$$\sigma(f_1 - i) = f_1 e + j - (i + j) = (f_1 - i)e \bmod \mathcal{J}^{n+1}_{CMK(p)},$$

using that $ie = i \bmod \mathcal{J}^{n+1}_{CMK(p)}$, and $S_{CM,n+1} \neq \emptyset$ because it contains $f_1 - i$.

Notice that each S_{CMn} is a finite set and each $f \in S_{CMn}$ has a finite field of definition. This follows from the fact that for any $C, M, n \in \mathbb{N}$, the $\mathbb{Z}_p$-module $\mathcal{A}_{CM} \operatorname{mod} \mathcal{J}_{CM}^n$ has finitely many free generators and, therefore, the equation $\sigma f = fe$ is equivalent to finitely many usual polynomial equations. Also notice that $\{S_{CMn} \mid C, M, n \in \mathbb{N}\}$ has a natural structure of projective system. Therefore, $\varprojlim_{C,M,n} CMn \neq \emptyset$, and any element f of this projective limit satisfies $f \in 1 + \mathcal{J}_{K(p)}$ and $\sigma(f) = fe$.

The proposition is proved. □

For any $f \in 1 + \mathcal{J}_{K(p)}$ such that $\sigma(f) = fe$ and $\tau \in \Gamma(p)$, set $\psi_f(\tau) = (\tau f) f^{-1}$. Clearly, $\sigma(\psi_f(\tau)) = \tau(\sigma f)(\sigma f)^{-1} = (\tau f) e e^{-1} f = \psi_f(\tau)$. Therefore, $\psi_f(\tau) \in (1 + \mathcal{J}_{K(p)})|_{\sigma = \mathrm{id}} = 1 + \mathcal{J}$.

Proposition 1.2. a) *ψ_f is a closed group embedding of $\Gamma(p)$ into $(1+\mathcal{J})^{\times}$.*
b) *ψ_f induces an isomorphism ψ_f^{ab} of the topological groups $\Gamma(p)^{\mathrm{ab}}$ and $(1+\mathcal{J})^{\times} \operatorname{mod} \mathcal{J}^2$.*
c) *If $f_1 \in 1 + \mathcal{J}_{K(p)}$ is such that $\sigma(f_1) = f_1 e$ then there is an element $c \in 1 + \mathcal{J}$ such that for any $\tau \in \Gamma(p)$, $\psi_{f_1}(\tau) = c\psi_f(\tau)c^{-1}$.*
d) *ψ_f induces an embedding of the group of all continuous automorphisms* $\mathrm{Aut}\Gamma(p)$ *into the group* $\mathrm{Aut}\mathcal{A}$ *of continuous automorphisms of the $\mathbb{Z}_p$-algebra $\mathcal{A}$.*

Proof. a) Clearly, ψ_f can be treated as a pro-p-version of the embedding of the group $\Gamma(p)$ into its Magnus algebra. Therefore, by [8], Ch 1, Sec 6, ψ_f induces, for all $n \in \mathbb{N}$, the closed embeddings of the quotients $C_n(\Gamma(p))/C_{n+1}(\Gamma(p))$ of commutator subgroups in $\Gamma(p)$ into $1 + \mathcal{J}^n \operatorname{mod} \mathcal{J}^{n+1}$. This implies that ψ_f induces, for all $n \geqslant 1$, the closed group embeddings of $\Gamma(p)/C_n(\Gamma(p))$ into $1 + \mathcal{J} \operatorname{mod} \mathcal{J}^n$, and therefore, ψ_f is a closed group monomorphism.

b) Consider the profinite $\mathbb{Z}_p$-basis $\{D_a^{(r)} \mid a \in \mathbb{Z}(p), 1 \leqslant r \leqslant N_0\} \cup \{D_0\}$ for $\mathcal{J} \operatorname{mod} \mathcal{J}^2$ from n.1.2. For $1 \leqslant r \leqslant N_0$, as earlier, consider $\alpha_r \in W(k)$, which form the dual basis of the basis $\{\beta_r \mid 1 \leqslant r \leqslant N_0\}$ chosen in n.1.2 to define the generators $D_a^{(r)}$. Then

$$e = 1 + \sum_{1 \leqslant r \leqslant N_0 a \in \mathbb{Z}(p)} \alpha_r t^{-a} D_a^{(r)} + \alpha_0 D_0$$

and

$$f = 1 + \sum_{1 \leqslant r \leqslant N_0 a \in \mathbb{Z}(p)} f_a^{(r)} D_a^{(r)} + f_0 D_0 \operatorname{mod} \mathcal{J}_{K(p)}^2,$$

where for $1 \leqslant r \leqslant N_0$ and $a \in \mathbb{Z}(p)$, $f_a^{(r)}$ and f_0 belong to $O(K(p)) \subset W(K(p))$ and satisfy the equations $\sigma f_a^{(r)} - f_a^{(r)} = \alpha_r t^{-a}$ and $\sigma f_0 - f_0 = \alpha_0$.

Then for any $\tau \in \Gamma(p)$,

$$\psi_f(\tau) = 1 + \sum_{a,r} (\tau f_a^{(r)} - f_a^{(r)}) D_a^{(r)} + (\tau f_0 - f_0) D_0 \bmod \mathcal{J}_{K(p)}^2$$

and the identification $\psi_f : \Gamma(p)^{\mathrm{ab}} \simeq (1 + \mathcal{J})^\times \bmod \mathcal{J}^2$ is equivalent to the identifications of Witt-Artin-Schreier theory

$$\oplus_{a \in \mathbb{Z}(p)} W(k) t^{-a} \oplus W(\mathbb{F}_p)\alpha_0 = O(K)/(\sigma - \mathrm{id})O(K) = \mathrm{Hom}_{\mathrm{cts}}(\Gamma(p), W(\mathbb{F}_p)).$$

c) Clearly, $\sigma(f_1 f^{-1}) = \sigma(f_1)\sigma(f)^{-1} = f_1 e e^{-1} f^{-1} = f_1 f^{-1}$. Therefore,

$$f_1 f^{-1} = c \in (1 + \mathcal{J}_{K(p)}) \cap \mathcal{A} = 1 + \mathcal{J}$$

and for any $\tau \in \Gamma(p)$,

$$\psi_{f_1}(\tau) = \tau(f_1) f_1^{-1} = \tau(cf)(cf)^{-1} = c(\tau f) f^{-1} c^{-1} = c\psi_f(\tau) c^{-1}.$$

d) This also follows from the above mentioned interpretation of $\mathcal{A}$ as a profinite analogue of the Magnus algebra for $\Gamma(p)$. □

1.4. The identification ψ_f^{ab}. As it was already mentioned in the proof of proposition 1.2 the identification ψ_f^{ab} comes from the isomorphism of Witt-Artin-Schreier theory

$$\Gamma(p)^{\mathrm{ab}} = \mathrm{Hom}(O(K)/(\sigma - \mathrm{id})O(K), W(\mathbb{F}_p))$$

and does not depend on the choice of $t = t_K$ and $f \in 1 + \mathcal{J}_{K(p)}$. Suppose $\tau_0 \in \Gamma(p)^{\mathrm{ab}}$ is such that $\psi_f^{\mathrm{ab}}(\tau_0) = 1 + D_0$ and for $a \in \mathbb{Z}(p)$ and $1 \leqslant r \leqslant N_0$, the elements $\tau_a^{(r)} \in \Gamma(p)^{\mathrm{ab}}$ are such that $\psi_f^{\mathrm{ab}}(\tau_a^{(r)}) = 1 + D_a^{(r)} \bmod \mathcal{J}^2$. Then the element

$$e = 1 + \alpha_0 D_0 + \sum_{a,r} \alpha_r t^{-a} D_a^{(r)}$$

corresponds to the diagonal element $\alpha_0 \otimes \tau_0 + \sum_{a,r} \alpha_r t^{-a} \otimes \tau_a^{(r)}$ from $O(K) \otimes \Gamma(p)^{\mathrm{ab}} =$

$$O(K) \otimes \mathrm{Hom}(O(K)/(\sigma - \mathrm{id})O(K), \mathbb{Z}_p) = \mathrm{Hom}(O(K)/(\sigma - \mathrm{id})O(K), O(K)),$$

which comes from the following natural embedding

$$O(K)/(\sigma - \mathrm{id})O(K) = \oplus_{a \in \mathbb{Z}(p)} W(k) t^{-a} \oplus W(\mathbb{F}_p)\alpha_0 \subset O(K).$$

The above elements τ_0, resp. $\tau_a^{(r)}$, correspond to t, resp. $E(\beta_r, t^a)^{1/a}$, by the reciprocity map of local class field theory. (Here $\beta_1, \dots, \beta_{N_0} \in W(k)$ were chosen in n.1.2 and for $\beta \in W(k)$,

$$E(\beta, X) = \exp(\beta X + (\sigma\beta) X^p / p + \dots + (\sigma^n \beta) X^{p^n} / p^n + \dots) \in W(k)[[X]]$$

is the generalisation of the Artin-Hasse exponential introduced by Shafarevich [9].) This fact follows from the Witt explicit reciprocity law, cf. [5]. Then the elements D_{an}, where $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\operatorname{mod} N_0$, correspond to

$$\sum_{1\leqslant r\leqslant N_0}\sigma^n(\alpha_r)\otimes E(\beta_r,t^a)^{1/a}\in W(k)\otimes_{\mathbb{Z}_p}\mathcal{G}_a,$$

where the (multiplicative) group $\mathcal{G}_a:=\{E(\gamma,t^a)\mid\gamma\in W(k)\}$ is identified with the $\mathbb{Z}_p$-module of Witt vectors $W(k)$ via the map $E(\gamma,t^a)^{1/a}\mapsto\gamma$. Consider the identification

$$W(k)\otimes_{\mathbb{Z}_p}W(k)=\oplus_{m\in\mathbb{Z}\operatorname{mod}N_0}W(k)_m$$

given by the correspondence $\alpha\otimes\beta\mapsto\{\sigma^{-m}(\alpha)\beta\}_{m\in\mathbb{Z}\operatorname{mod}N_0}$. Under this identification the element D_{an} corresponds to the vector $\delta_n\in\oplus_m W(k)_m$, which has n-th coordinate 1 and all remaining coordinates 0. This interpretation of the generators D_{an} will be applied below in the following situation. Suppose $[k':k]<\infty$, $k'\simeq\mathbb{F}_{q_0'}$ with $q_0'=p^{N_0'}$. Clearly, $N_0'\equiv 0\operatorname{mod}N_0$. For $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\operatorname{mod}N_0'$ denote by D'_{an} an analogue of D_{an} constructed for $K'=k'((t_{K'}))$ with $t_{K'}=t$. Let $\Gamma'=\operatorname{Gal}(K_{\mathrm{sep}}/K')$ and let $\Gamma'(p)$ be the Galois group of the maximal p-extension $K'(p)$ of K' in K_{sep}. With the above notation we have the following property:

Proposition 1.3. *For any $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\operatorname{mod}N_0'$, D'_{an} is mapped to $D_{a,n\operatorname{mod}N_0}$ under the map $\Gamma'(p)^{\mathrm{ab}}\longrightarrow\Gamma(p)^{\mathrm{ab}}$, which is induced by the natural embedding $\Gamma'\subset\Gamma$.*

2. Action of analytic automorphisms on $I^{\mathrm{ab}}(p)$

As earlier, $K=k((t))$, $k\simeq\mathbb{F}_{q_0}$ with $q_0=p^{N_0}$ and $\Gamma(p)=\operatorname{Gal}(K(p)/K)$. Let $I(p)$ be the inertia subgroup of $\Gamma(p)$ and let $I(p)^{\mathrm{ab}}$ be its image in the maximal abelian quotient $\Gamma(p)^{\mathrm{ab}}$ of $\Gamma(p)$.

2.1. Consider the group $\operatorname{Aut}K$ of continuous field automorphisms of K. Let $\operatorname{Fr}(t)\in\operatorname{Aut}K$ be such that $\operatorname{Fr}(t)|_k=\sigma$ and $\operatorname{Fr}(t):t\mapsto t$. Then any element of $\operatorname{Aut}K$ is the composition of a power $\operatorname{Fr}(t)^n$, where $n\in\mathbb{Z}\operatorname{mod}N_0$, and a field automorphism from $\operatorname{Aut}^0(K):=\{\eta\in\operatorname{Aut}K\mid\eta|_k=\mathrm{id}\}$. Notice that any $\eta\in\operatorname{Aut}^0K$ is uniquely determined by the image $\eta(t)$ of t, which is again a uniformizer in K.

Let $\operatorname{Aut}_K K(p)$ be the group of continuous automorphisms $\bar\eta$ of $K(p)$ such that $\bar\eta|_K\in\operatorname{Aut}K$. Then $\operatorname{Aut}_K K(p)$ acts on $\Gamma(p)$: if $\bar\eta\in\operatorname{Aut}_K K(p)$ and $\tau\in\Gamma(p)$ then the action of $\bar\eta$ is given by the correspondence $\tau\mapsto\bar\eta^*(\tau)=\bar\eta^{-1}\tau\bar\eta$, i.e. $\bar\eta^*(\tau):K(p)\xrightarrow{\bar\eta^{-1}}K(p)\xrightarrow{\tau}K(p)\xrightarrow{\bar\eta}K(p)$, cf. the introduction for the agreement about compositions of maps. The action induced by $\bar{\eta}^* \in \mathrm{Aut}_K K(p)$ on $\Gamma(p)^{\mathrm{ab}}$ depends only on $\eta := \bar{\eta}|_K$ and will be denoted simply by η^*.

2.2. Let $\mathcal{M} = I(p)^{\mathrm{ab}} \otimes \mathbb{F}_p$. If U_K is the group of principal units in K then we shall use the identification $\mathcal{M} = U_K/U_K^p$, which is given by the reciprocity map of local class field theory. Notice that, with respect of this identification, for any $\eta \in \mathrm{Aut}K$, the action η^* comes from the natural action of η on K. We shall denote the k-linear extension of the action of η to $\mathcal{M}_k := \mathcal{M} \otimes_{\mathbb{F}_p} k$ by the same symbol η^*.

Use the map $m \mapsto (\psi_f^{\mathrm{ab}}(m) - 1) \bmod p$ to identify $\mathcal{M}_k$ with a submodule of $\mathcal{J}_k \bmod(p, \mathcal{J}_k^2)$. For $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z} \bmod N_0$, consider the images of the elements D_{an}, where $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z} \bmod N_0$ (cf. n.1), in $\mathcal{J}_k \bmod(p, \mathcal{J}_k^2)$. Denote these images by same symbols. Then they give a set of free topological generators of the k-module $\mathcal{M}_k$. The action of $\eta \in \mathrm{Aut}K$ on $\mathcal{M}_k$ in terms of these generators is as follows.

Proposition 2.1. 1) $\mathrm{Fr}(t)^*(D_{an}) = D_{a,n-1}$*;*
2) *if* $\eta \in \mathrm{Aut}^0 K$*, then*

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

Proof. 1) Consider the generators $\alpha_r D_a^{(r)}$ of $\mathcal{A}$ from n.1.2, where $a \in \mathbb{Z}(p), 1 \leqslant r \leqslant N_0$. Note that the residue of the corresponding element $e - 1$ modulo $(\sigma - \mathrm{id})K \otimes (\mathcal{J} \bmod \mathcal{J}^2)$ does not depend on the choice of t or of the elements $\alpha_1, \alpha_2, \dots, \alpha_{N_0}$, because this is the diagonal element of Artin-Schreier duality. Therefore, if $\mathrm{Fr}(t)^*(D_a^{(r)}) = D_a'^{(r)}$ and $\mathrm{Fr}(t)^*(D_0) = D_0'$ then

$$\begin{aligned} e - 1 &\equiv \sigma(\alpha_0) \otimes D_0' + \sum_{a,r} \sigma(\alpha_r) t^{-a} \otimes D_a'^{(r)} \\ &\equiv \alpha_0 \otimes D_0 + \sum_{a,r} \alpha_r t^{-a} \otimes D_a^{(r)} \bmod (\sigma - \mathrm{id})K \otimes (\mathcal{J} \bmod \mathcal{J}^2). \end{aligned} \tag{2.1}$$

So, for any $a \in \mathbb{Z}(p)$, we see that in $k \otimes_{\mathbb{F}_p} \mathcal{M} = \mathcal{M}_k$

$$D_{a0} = \sum_r \alpha_r \otimes D_a^{(r)} = \sum_r \sigma(\alpha_r) \otimes D_a'^{(r)}.$$

Denoting the k-linear extension of $\mathrm{Fr}(t)^*$ by the same symbol, as usual, we have

$$\mathrm{Fr}(t)^*(D_{a0}) = \sum_r \alpha_r \otimes \mathrm{Fr}(t)^*(D_a^{(r)}) = \sum_r \alpha_r \otimes D_a'^{(r)} = \sigma^{-1} D_{a0} = D_{a,-1}.$$

Therefore, for any $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z} \bmod N_0$, $\mathrm{Fr}(t)^*(D_{an}) = D_{a,n-1}$. Notice also that congruence (2.1) implies that $\mathrm{Fr}(t)^* D_0 = D_0$.

2) Using that η is a k-linear automorphism of K and proceeding similarly to the above part 1) we obtain that

$$\sum_{a\in\mathbb{Z}(p)^0}\eta(t)^{-a}\eta^*(D_{a0})\equiv\sum_{a\in\mathbb{Z}(p)^0}t^{-a}D_{a0}\,\mathrm{mod}(\sigma-\mathrm{id})K\otimes\mathcal{M}.$$

Now apply $(\eta^{-1}\otimes\mathrm{id})$ to both sides of this congruence and notice that we can omit the terms with index $a=0$ when working modulo $(k+(\sigma-\mathrm{id})K)\otimes\mathcal{M}$, because they belong to $\mathcal{M}_k$. The lemma is proved. □

2.3. If f is a continuous automorphism of the $\mathbb{F}_p$-module $\mathcal{M}$, we agree to use the same notation f for its k-linear extension to an automorphism of $\mathcal{M}_k$. For any $a\in\mathbb{Z}(p)$, set

$$f(D_{a0})=\sum_{\substack{b\in\mathbb{Z}(p)\\ n\in\mathbb{Z}\,\mathrm{mod}\,N_0}}\alpha_{abn}(f)D_{bn}.$$

Then all coefficients $\alpha_{abn}(f)$ are in k. Sometimes we shall use the notation $\alpha_{abn}(f)$ if a or b are divisible by p, then it is assumed that $\alpha_{abn}(f)=0$. Notice that for any $m\in\mathbb{Z}\,\mathrm{mod}\,N_0$,

$$f(D_{am})=\sum_{\substack{b\in\mathbb{Z}(p)\\ n\in\mathbb{Z}\,\mathrm{mod}\,N_0}}\sigma^m(\alpha_{abn}(f))D_{b,n+m}.$$

Definition. For any $v\in\mathbb{N}$, let $\mathcal{M}^{(v)}$ be the minimal closed $\mathbb{F}_p$-submodule in $\mathcal{M}$ such that $\mathcal{M}_k^{(v)}:=\mathcal{M}^{(v)}\otimes k$ is topologically generated over k by all D_{an}, where $a\in\mathbb{Z}(p)$, $a\geqslant v$ and $n\in\mathbb{Z}\,\mathrm{mod}\,N_0$. (Notice that $\mathcal{M}=\mathcal{M}^{(1)}$.)

Definition. $\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ is the subset in the group $\mathrm{Aut}\mathcal{M}$, consisting of all continuous $\mathbb{F}_p$-linear automorphisms f satifying $\alpha_{a,b,m\,\mathrm{mod}\,N_0}(f)=0$ if $bp^m<a$, for any $a,b\in\mathbb{Z}(p)$ and $-N_0<m\leqslant 0$.

It is easy to see that:

(1) $\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ is a subgroup of $\mathrm{Aut}\mathcal{M}$;

(2) if $f\in\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ then for any $a\in\mathbb{N}$, $f(\mathcal{M}^{(a)})\subset\mathcal{M}^{(a)}$, i.e. f is compatible with the image of the ramification filtration in $\mathcal{M}$;

(3) if $f\in\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ then for any $a\in\mathbb{Z}(p)$, $\alpha_{aa0}\in k^*$ and $\alpha_{aan}(f)=0$ if $n\neq 0$.

Definition. For $f\in\mathrm{Aut}\mathcal{M}$, let $f_{\mathrm{an}}\in\mathrm{End}\,\mathcal{M}$ be such that for all $a\in\mathbb{Z}(p)$,

$$f_{\mathrm{an}}(D_{a0})=\sum_{b\in\mathbb{Z}(p)}\alpha_{ab0}(f)D_{b0}.$$

Proposition 2.2. *If $f, g \in \mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ then for any $a, b \in \mathbb{Z}(p)$ such that $a \leqslant b < ap^{N_0}$,*

$$\alpha_{ab0}(fg) = \sum_c \alpha_{ac0}(f)\alpha_{cb0}(g).$$

Corollary 2.3. *If $v < p^{N_0}$ then the correspondence $f \mapsto f_{\mathrm{an}}$ is a group homomorphism from $\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ to $\mathrm{Aut}_{\mathrm{adm}}\mathcal{M} \bmod \mathcal{M}^{(v)}$.*

Proof. We have $\alpha_{ab0}(fg) =$

$$\sum_{\substack{m+n\equiv 0 \bmod N_0 \\ 0\geqslant n,m>-N_0}} \alpha_{a,c,n \bmod N_0}(f)\sigma^n(\alpha_{c,b,m \bmod N_0}(g))D_{b,(m+n) \bmod N_0}.$$

Then $\alpha_{a,c,n \bmod N_0}(f) \neq 0$ implies that $cp^n \geqslant a$ and $\alpha_{c,b,m \bmod N_0}(g) \neq 0$ implies that $bp^m \geqslant c$. So, if the corresponding coefficient for $D_{b,(m+n) \bmod N_0}$ is not zero then $bp^{m+n} \geqslant a$, i.e. $m+n > -N_0$ and, therefore, $m = n = 0$. □

The following proves that $\mathrm{Aut}^0 K \subset \mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$.

Proposition 2.4. *If $\eta \in \mathrm{Aut}^0 K$ then $\eta^* \in \mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$.*

Proof. For $a \in \mathbb{Z}(p)$, set

$$\eta^{-1}(t)^{-a} \equiv \sum_{\substack{b\in\mathbb{Z}(p) \\ s\geqslant 0}} \gamma_{abs} t^{-bp^s} \bmod k[[t]].$$

Clearly, $\gamma_{abs} = 0$ if $bp^s > a$. It follows from part 2) of proposition 2.1 that

$$\eta^*(D_{b0}) = \sum_{\substack{a\in\mathbb{Z}(p) \\ s\geqslant 0}} \sigma^{-s}(\gamma_{abs})D_{a,-s \bmod N_0}.$$

Therefore, for $0 \leqslant m < N_0$,

$$\alpha_{b,a,-m \bmod N_0}(\eta^*) = \sum_{\substack{s\equiv m \bmod N_0 \\ s\geqslant 0}} \sigma^{-s}(\gamma_{abs})$$

and $a/p^m < b$ implies for $s \equiv m \bmod N_0$, $s \geqslant 0$, that $a/p^s < b$. So, $bp^s > a$, $\gamma_{abs} = 0$ and $\alpha_{b,a,-m \bmod N_0}(\eta^*) = 0$.

The proposition is proved. □

2.4. In this subsection we prove three technical propositions. Notice that in proposition 2.5 we treat the case of fields of characteristic $p \neq 2$ and in proposition 2.6 the characteristic of K is 2. Propositions 2.5-2.7 will be used later in section 5. If $a, b \in \mathbb{N}$ then δ_{ab} is the Kronecker symbol.

Proposition 2.5. *Suppose $p \neq 2$, $w_0 \in \mathbb{N}$, $w_0+1 \leqslant p^{N_0}$ and $f \in \mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ is such that $\alpha_{1a0}(f) = \delta_{1a}$ if $1 \leqslant a < w_0$ and $\alpha_{2a0}(f) = 0$ if $a \equiv 1 \bmod p$ and $a \leqslant w_0$. Then there is an $\eta \in \mathrm{Aut}^0 K$ such that $\eta(t) \equiv t \bmod t^{w_0}$, $\alpha_{1a0}(f\eta^*) = \delta_{1a}$ if $1 \leqslant a < w_0 + 1$, and $\alpha_{2a0}(f\eta^*) = 0$ if $a \equiv 1 \bmod p$ and $a \leqslant w_0 + 1$.*

Proof. Take $\eta\in\mathrm{Aut}^0K$ such that $\eta^{-1}(t)=t(1+\gamma t^{w_0-1})$ with $\gamma\in k$. Then for any $a\in\mathbb{Z}(p)$, $\eta^{-1}(t^{-a})=t^{-a}(1-a\gamma t^{w_0-1})\,\mathrm{mod}\,t^{-a+w_0}$, and part 2) of proposition 2.1 implies that $\alpha_{aa0}(\eta^*)=1$, $\alpha_{ab0}(\eta^*)=0$ if $a<b<a+w_0-1$, $\alpha_{a,a+w_0-1,0}(\eta^*)=-(a+w_0-1)\gamma$.

Therefore, by proposition 2.2 $\alpha_{1a0}(f\eta^*)=\delta_{1a}$ if $1\leqslant a<w_0$ and $\alpha_{2a0}(f\eta^*)=0$ if $a\equiv 1\,\mathrm{mod}\,p$, $a\leqslant w_0$.

Suppose $w_0\not\equiv 0\,\mathrm{mod}\,p$. Then by proposition 2.2

$$\alpha_{1w_00}(f\eta^*)=-w_0\gamma+\alpha_{1w_00}(f)=0$$

if $\gamma=w_0^{-1}\alpha_{1w_00}(f)$. This proves the proposition in the case $w_0\not\equiv 0\,\mathrm{mod}\,p$, because $w_0+1\not\equiv 1\,\mathrm{mod}\,p$ and no conditions are required for $\alpha_{2,w_0+1,0}(f\eta^*)$.

Suppose $w_0\equiv 0\,\mathrm{mod}\,p$. Then there are no conditions for $\alpha_{1w_00}(f\eta^*)$ and by proposition 2.2

$$\begin{aligned}\alpha_{2,w_0+1,0}(f\eta^*)&=\alpha_{220}(f)\alpha_{2,w_0+1,0}(\eta^*)+\alpha_{2,w_0+1,0}(f)\alpha_{w_0+1,w_0+1,0}(\eta^*)\\&=-\alpha_{220}(f)\gamma+\alpha_{2,w_0+1,0}(f)=0\end{aligned}$$

if $\gamma=\alpha_{2,w_0+1,0}(f)\alpha_{220}(f)^{-1}$. (Using that $f\in\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ hence $\alpha_{220}(f)\in k^*$.)

The proposition is proved. □

Proposition 2.6. *Let $M\in\mathbb{N}$, $p=2$, $w_0=4M$ and $w_0+1<2^{N_0}$. Suppose $f\in\mathrm{Aut}_{\mathrm{adm}}\mathcal{M}$ is such that $\alpha_{1a0}(f)=\delta_{1a}$ if $1\leqslant a\leqslant w_0-3$ and $\alpha_{3a0}(f)=\delta_{3a}$ if $3\leqslant a\leqslant w_0-1$. Then there is an $\eta\in\mathrm{Aut}^0K$ such that $\alpha_{1a0}(f\eta^*)=\delta_{1a}$ and $\alpha_{3a0}(f\eta^*)=\delta_{3a}$ if $a\leqslant w_0+1$.*

Proof. 1st step.

Take $\eta_1\in\mathrm{Aut}^0K$ such that $\eta_1^{-1}(t)=t(1+\gamma_1t^{4M-2})$ with $\gamma_1\in k$. Then for $a\in\mathbb{Z}(2)$, $\eta_1^{-1}(t^{-a})\equiv t^{-a}(1+\gamma_1t^{4M-2})\,\mathrm{mod}\,t^{-a+4M}$ and by part 2) of proposition 2.1, $\alpha_{aa0}(\eta_1^*)=1$, $\alpha_{ab0}(\eta_1^*)=0$ if $a<b<a+4M-2$, and $\alpha_{a,a+4M-2,0}(\eta_1^*)=\gamma_1$.

So by proposition 2.2, $\alpha_{1a0}(f\eta_1^*)=\alpha_{1a0}(f)$ if $a\leqslant 4M-3=w_0-3$, $\alpha_{3a0}(f\eta_1^*)=\alpha_{3a0}(f)$ if $a\leqslant 4M-1=w_0-1$, $\alpha_{1,w_0-1,0}(f\eta_1^*)=\alpha_{1,w_0-1,0}(f)+\alpha_{1,w_0-1,0}(\eta_1^*)=0$ if $\gamma_1=\alpha_{1,w_0-1,0}(f)$.

2nd step.

By the above first step we can now assume that $\alpha_{1,w_0-1,0}(f)=0$.

Take $\eta_2\in\mathrm{Aut}^0K$ such that $\eta_2^{-1}(t)=t(1+\gamma_2t^{2M-1})$. Then for $a\in\mathbb{Z}(2)$, $\eta_2^{-1}(t^{-a})\equiv t^{-a}(1+\gamma_2t^{2M-1}+\delta(a)\gamma_2^2t^{4M-2})\,\mathrm{mod}\,t^{-a+4M}$, where $\delta(a)=a(a+1)/2$.

So by part 2) of proposition 2.1, $\alpha_{aa0}(\eta_2^*)=1$, $\alpha_{ab0}(\eta_2^*)=0$ if $a<b<a+4M-2$ (notice that $-a+2M-1\equiv 0\,\mathrm{mod}\,2$), and $\alpha_{a,a+4M-2,0}(\eta_2^*)=\delta(a+4M-2)\gamma_2^2$ (notice that $\delta(a+4M-2)=0$ if $a\equiv 1\,\mathrm{mod}\,4$ and $\delta(a+4M-2)=1$ if $a\equiv 3\,\mathrm{mod}\,4$).

Again by proposition 2.2, $\alpha_{1a0}(f\eta_2^*) = \alpha_{1a0}(f)$ if $a \leqslant 4M-1 = w_0-1$ (use that $\alpha_{1,w_0-1,0}(f) = \alpha_{1,w_0-1,0}(\eta_2^*) = 0$), $\alpha_{3a0}(f\eta_2^*) = \alpha_{3a0}(f)$ if $a \leqslant 4M-1 = w_0-1$, $\alpha_{3,w_0+1,0}(f\eta_2^*) = \alpha_{3,w_0+1,0}(f) + \alpha_{3,w_0+1,0}(\eta_2^*) = 0$ if $\gamma_2 \in k$ is such that $\gamma_2^2 = \alpha_{3,w_0+1,0}(f)$.

3rd step.

Now we can assume that $\alpha_{1,w_0-1,0}(f) = \alpha_{3,w_0+1,0}(f) = 0$.

Take $\eta_3 \in \mathrm{Aut}^0 K$ such that $\eta_3^{-1}(t) = t(1+\gamma_3 t^{4M})$. Then for $a \in \mathbb{Z}(2)$, $\eta_3^{-1}(t^{-a}) \equiv t^{-a}(1+\gamma_3 t^{4M}) \bmod t^{-a+4M+2}$, $\alpha_{aa0}(\eta_3^*) = 1$, $\alpha_{ab0}(\eta_3^*) = 0$ if $a < b < a+4M$, and $\alpha_{a,a+4M,0}(\eta_3^*) = \gamma_3$.

This implies that $\alpha_{1a0}(f\eta_3^*) = \alpha_{1a0}(f)$ if $a \leqslant 4M-1 = w_0-1$, $\alpha_{1,w_0+1,0}(f\eta_3^*) = \alpha_{1,w_0+1,0}(f) + \alpha_{1,w_0+1,0}(\eta_3^*) = 0$ if $\gamma_3 = \alpha_{1,w_0+1,0}(f)$ and $\alpha_{3a0}(f\eta_3^*) = \alpha_{3a0}(f)$ if $a \leqslant w_0+1$.

The proposition is proved. □

Proposition 2.7. *Suppose $a \in \mathbb{Z}(p)$, $w_0 \leqslant ap^{N_0}$, where $w_0 \in p\mathbb{N}$, $w_0 > a+1$ if $p \neq 2$ and $w_0 \in 4\mathbb{N}$, $w_0 > a+2$ if $p = 2$. Suppose $\eta, \eta_1 \in \mathrm{Aut}^0 K$ are such that for any $b, c \in \mathbb{Z}(p)$ satisfying the restrictions $a \leqslant c \leqslant b < w_0 \leqslant ap^{N_0}$, we have the equality*

$$\alpha_{cb0}(\eta^*) = \alpha_{cb0}(\eta_1^*).$$

Then $\eta(t) \equiv \eta_1(t) \bmod t^{v_0}$, where $v_0 = w_0 - a + 1$ if $p \neq 2$ and $v_0 = (w_0-a+1)/2$ if $p = 2$.

Remark. With notation from Subsection 2.3 this proposition implies that if ${\eta_1}_{\mathrm{an}}^* \equiv \eta_{\mathrm{an}}^* \bmod \mathcal{M}^{(w_0)}$ then $\eta(t) \equiv \eta_1(t) \bmod t^{v_0}$.

Proof. Use proposition 2.2 to reduce the proof to the case $\eta_1(t) = t$.

Suppose, first, that $\eta^{-1}(t) = \alpha t \bmod t^2$. Then

$$\alpha_{cc0}(\eta^*) = \alpha^{-c} = 1. \tag{2.2}$$

If $a+1 \in \mathbb{Z}(p)$ then $p \neq 2$ and we can use formula (2.2) for $c = a, a+1$ to prove that $\alpha = 1$. Suppose $a+1 \notin \mathbb{Z}(p)$. If $p = 2$ use (2.2) for $c = a, a+2 < w_0$, and if $p \neq 2$ use (2.2) for $c = a+2, a+3 < w_0$ to prove again that $\alpha = 1$.

Assume now that $p \neq 2$.

Suppose $\eta^{-1}(t) \equiv t + \alpha t^{v-1} \bmod t^v$ with $v \geqslant 3$ and $\alpha \in k^*$. If $a+v-2 \in \mathbb{Z}(p)$ then by part 2) of proposition 2.1 $\alpha_{a,a+v-2,0}(\eta^*) \neq 0$. This implies that $a+v-2 \geqslant w_0+1$, i.e. $v \geqslant w_0-a+1$, as required. If $a+v-2 \equiv 0 \bmod p$ then by part 2) of proposition 2.1 $\alpha_{a+1,a+v-1,0}(\eta^*) \neq 0$.This implies that $a+v-1 \geqslant w_0+1$ and $v \geqslant w_0-a+2 > w_0-a+1$. The case $p \neq 2$ is considered.

Assume now that $p = 2$.

Suppose that $M\in\mathbb{N}$ is such that

$$\eta^{-1}(t)=t\left(1+\sum_{r\geqslant 2M-1}\gamma_r t^r\right)\equiv t \bmod t^{2M}$$

with either $\gamma_{2M-1}\neq 0$ or $\gamma_{2M}\neq 0$.

Therefore, if $r\equiv 0 \bmod 2$, $r\geqslant 2M-1$ and $a+r<ap^{N_0}$ then by part 2) of proposition 2.1 $\alpha_{a,a+r,0}(\eta^*)=\gamma_r$. This implies that either $2M\geqslant w_0$ (and the proposition is proved) or $2M\leqslant w_0-2$, $\gamma_{2M}=0$ and $\gamma_{2M-1}\neq 0$.

Suppose $a+4M<w_0$. Then with the notation from the second step in the proof of proposition 2.6, we have

$$\alpha_{a,a+4M-2,0}(\eta^*)=\gamma_{4M-2}+\gamma_{2M-1}^2\delta(a+4M-2)$$
$$\alpha_{a+2,a+4M,0}(\eta^*)=\gamma_{4M-2}+\gamma_{2M-1}^2\delta(a+4M).$$

The sum of the right hand sides of the above two equalities is $\gamma_{2M-1}^2\neq 0$, because $\delta(a+4M-2)+\delta(a+4M)=1$. Therefore, at least one of their left hand sides is not zero. This means that the assumption about $a+4M<w_0$ was wrong. Therefore, $4M>w_0-a$ and $2M\geqslant (w_0-a+1)/2$.

The proposition is proved. □

3. Compatible systems of group morphisms

For any $s\in\mathbb{Z}_{\geqslant 0}$, let K_s be the unramified extension of K in $K(p)$ of degree p^s. Then $K_s=k_s((t))$, where $t=t_K$ is a fixed uniformiser, $k\subset k_s$, $[k_s:k]=p^s$, $k_s\simeq\mathbb{F}_{q_s}$, $q_s=p^{N_s}$ with $N_s=N_0p^s$.

Let K_{ur} be the union of all K_s, $s\geqslant 0$. This is the maximal unramified extension of K in $K(p)$ and its residue field coincides with the residue field $k(p)$ of $K(p)$. Let $I_{K_{\mathrm{ur}}}(p)^{\mathrm{ab}}$, resp. $I_{K_s}(p)^{\mathrm{ab}}$, for $s\in\mathbb{Z}_{\geqslant 0}$, be the images of the inertia subgroups of $\mathrm{Gal}(K(p)/K_{\mathrm{ur}})$, resp. $\mathrm{Gal}(K(p)/K_s)$, in the corresponding maximal abelian quotients. Then $I_{K_{\mathrm{ur}}}(p)^{\mathrm{ab}}=\varprojlim_s I_{K_s}(p)^{\mathrm{ab}}$.

3.1. For $s\geqslant 0$, introduce the $\mathbb{F}_p$-modules $\mathcal{M}_{Ks}=I_{K_s}(p)^{\mathrm{ab}}\otimes\mathbb{F}_p$ and $\mathcal{M}_{K\mathrm{ur}}=I_{K_{\mathrm{ur}}}(p)^{\mathrm{ab}}\otimes\mathbb{F}_p$ with the corresponding $k(p)$-modules $\bar{\mathcal{M}}_{Ks}=\mathcal{M}_{Ks}\hat{\otimes}_{\mathbb{F}_p}k(p)$ and $\bar{\mathcal{M}}_{K\mathrm{ur}}=\mathcal{M}_{K\mathrm{ur}}\hat{\otimes}_{\mathbb{F}_p}k(p)$. Then for all $s\geqslant 0$, we have natural connecting morphisms $j_s:\mathcal{M}_{K,s+1}\longrightarrow\mathcal{M}_{Ks}$ and $\bar{j}_s:\bar{\mathcal{M}}_{K,s+1}\longrightarrow\bar{\mathcal{M}}_{Ks}$ (both are induced by the natural group embeddings $\Gamma_{K_{s+1}}\longrightarrow\Gamma_{K_s}$). Therefore, we have projective systems $\{\mathcal{M}_{Ks},j_s\}$ and $\{\bar{\mathcal{M}}_{Ks},\bar{j}_s\}$ and natural identifications $\mathcal{M}_{K\mathrm{ur}}=\varprojlim_s\mathcal{M}_{Ks}$ and $\bar{\mathcal{M}}_{K_{\mathrm{ur}}}=\varprojlim_s\bar{\mathcal{M}}_{K_s}$.

Let $\mathcal{M}_{K\infty}$ be the $k(p)$-submodule in $\bar{\mathcal{M}}_{K\mathrm{ur}}$ which is topologically generated by all $D_{an}^{\infty}:=\varprojlim_s D_{a,n \bmod N_s}^{(s)}$, where $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}$. Here for

$a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\bmod N_s$, $D_{an}^{(s)}$ are generators for $\bar{\mathcal{M}}_{Ks}$, which are analogues of the generators D_{an} introduced in Section 2 for the k-module $\mathcal{M}_k$. Notice that the generators $D_{an}^{(s)}$ depend on the choice of the uniformising element t in K.

Proposition 3.1. *The $k(p)$-submodule $\mathcal{M}_{K\infty}$ of $\bar{\mathcal{M}}_{K\mathrm{ur}}$ does not depend on the choice of t.*

Proof. Let t_1 be another uniformiser in K. Introduce $\eta\in\mathrm{Aut}^0(K_{\mathrm{ur}})$ such that $\eta(t)=t_1$. The proposition will be proved if we show that $\eta^*(\mathcal{M}_{K\infty})=\mathcal{M}_{K\infty}$.

For $s\geqslant 0$, let $\eta_s=\eta|_{K_s}\in\mathrm{Aut}^0K_s$. Then for $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\bmod N_s$,

$$\eta_s^*(D_{an}^{(s)})=\sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z}\bmod N_s}}\sigma^n\alpha_{abm}(\eta_s^*)D_{b,m+n}^{(s)},$$

where the coefficients $\alpha_{abm}(\eta_s^*)\in k_s$ satisfy the following compatibility conditions (using that $j_s(D_{an}^{(s)})=D_{a,n\bmod N_{s-1}}^{(s-1)}$):

if $a,b\in\mathbb{Z}(p)$ and $m\in\mathbb{Z}\bmod N_{s-1}$ then

$$\sum_{n\bmod N_{s-1}=m}\alpha_{abn}(\eta_s^*)=\alpha_{abm}(\eta_{s-1}^*).$$

By proposition 2.4, if $0\leqslant m<N_s$ and $b/p^m<a$ then $\alpha_{a,b,-m\bmod N_s}(\eta_s^*)=0$. Therefore, if s is such that $b/p^{N_s}<a$ then $\alpha_{a,b,-m}^{\infty}(\eta^*):=\alpha_{a,b,-m\bmod N_s}(\eta_s^*)$ does not depend on s and for any $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}_{\geqslant 0}$,

$$\eta^*(D_{an}^{\infty})=\sum_{b\in\mathbb{Z}(p),m\geqslant 0}\sigma^n\alpha_{a,b,-m}^{\infty}(\eta^*)D_{b,n-m}^{\infty}\in\mathcal{M}_{K\infty}.$$

The proposition is proved. □

3.2. Consider the identification of class field theory $I_{K_s}(p)^{\mathrm{ab}}=U_{K_s}$, where U_{K_s} is the group of principal units of K_s. Define the continuous morphism of topological $k(p)$-modules

$$\pi_{Ks}:\bar{\mathcal{M}}_{Ks}=I_{K_s}(p)^{\mathrm{ab}}\hat{\otimes}k(p)\longrightarrow\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}},$$

by $\pi_{Ks}(u\otimes\alpha)=\alpha\,\mathrm{d}(u)/u$ for $u\in U_{K_s}$ and $\alpha\in k(p)$. Here $\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$ is the completion of the module of differentials of the valuation ring $O_{K_{\mathrm{ur}}}$ with respect to the t-adic topology. Notice that for any $a\in\mathbb{Z}(p)$ and $0\leqslant n<N_s$,

$$D_{a,n\bmod N_s}^{(s)}=\sum_{0\leqslant i<N_s}u_i\otimes(\sigma^n\alpha_i\bmod p).$$

Here $\{\alpha_i \mid 1\leqslant i\leqslant N_s\}$ is a $\mathbb{Z}_p$-basis of $W(k_s)$. If $\{\beta_i \mid 1\leqslant i\leqslant N_s\}$ is its dual basis then for $1\leqslant i\leqslant N_s$, $u_i=E(\beta_i,t^a)^{1/a}$, cf. Subsection 1.4. Therefore,

$$\pi_{Ks}(D^{(s)}_{a,n \bmod N_s})=\left(\sum_{i\geqslant 0}t^{ap^{n+iN_s}}\right)\frac{\mathrm{d}(t)}{t}.$$

It is easy to see that $\pi_{K\mathrm{ur}}:=\varprojlim \pi_{Ks}$ is a continuous map from $\bar{\mathcal{M}}_{K\mathrm{ur}}$ to $\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$.

Notice that if $\bar n=\varprojlim(n_s \bmod N_s)\in\varprojlim_s \mathbb{Z}/N_s\mathbb{Z}$, where all $n_s\in[0,N_s)$ and if $D^{\infty}_{a\bar n}=\varprojlim_s D^{(s)}_{a,n_s \bmod N_s}$, for $a\in\mathbb{Z}(p)$, then $\pi_{K\mathrm{ur}}(D^\infty_{a\bar n})=0$ if $\bar n\notin\mathbb{Z}_{\geqslant 0}\subset\varprojlim \mathbb{Z}/N_s\mathbb{Z}$, and $\pi_{K\mathrm{ur}}(D^\infty_{an})=t^{ap^n-1}\,\mathrm{d}(t)$ if $\bar n=n\in\mathbb{Z}_{\geqslant 0}$.

Let $\pi_{K\infty}:=\pi_{K\mathrm{ur}}|_{\mathcal{M}_{K\infty}}$. Then one can easily prove the following proposition.

Proposition 3.2. 1) $\pi_{K\infty}:\mathcal{M}_{K\infty}\longrightarrow\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$ *is a continuous epimorphism of $k(p)$-modules;*
2) $\ker\pi_{K\infty}$ *is the $k(p)$-submodule in $\mathcal{M}_{K\infty}$ topologically generated by all D^∞_{an} with $n<0$.*

3.3. Admissible systems of group morphisms. Suppose $K'=k((t'))\subset K(p)$ has the same residue field as K. Using K' instead of K we can introduce analogues $\mathcal{M}_{K's}$, $\bar{\mathcal{M}}_{K's}$, $\mathcal{M}_{K'\infty}$, etc. of $\mathcal{M}_{Ks}$, $\bar{\mathcal{M}}_{Ks}$, $\mathcal{M}_{K\infty}$, etc.

Definition. $f_{KK'}=\{f_{KK's}\}_{s\geqslant 0}$ is a family of continuous morphisms of $\mathbb{F}_p$-modules $f_{KK's}:\mathcal{M}_{Ks}\longrightarrow\mathcal{M}_{K's}$ which are always assumed to be compatible, i.e. for all $s\geqslant 0$, $f_{KK',s+1}j'_s=j_sf_{KK's}$. Here $j_s:\mathcal{M}_{K,s+1}\longrightarrow\mathcal{M}_{Ks}$ and $j'_s:\mathcal{M}_{K',s+1}\longrightarrow\mathcal{M}_{K's}$ are connecting morphisms.

We shall denote the $k(p)$-linear extension of $f_{KK's}$ by the same symbol $f_{KK's}$. Set

$$f_{KK'\mathrm{ur}}:=\varprojlim_s f_{KK's}:\bar{\mathcal{M}}_{K\mathrm{ur}}\longrightarrow\bar{\mathcal{M}}_{K'\mathrm{ur}}.$$

Definition. With the above notation $f_{KK'}$ is called admissible if:
A1. There is a continuous $k(p)$-linear isomorphism $f_{KK'\infty}:\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}\longrightarrow\hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}$ such that $f_{KK'\mathrm{ur}}\pi_{K'\mathrm{ur}}=\pi_{K\mathrm{ur}}f_{KK'\infty}$;
A2. $f_{KK'\infty}$ commutes with the Cartier operators C and C' on $\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$ and, resp., $\hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}$;
A3. For all $m\in\mathbb{N}$, $f_{KK'\infty}\left(t^m\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}\right)\subset t'^m\hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}$.

Remark. Recall that the Cartier operator $C:\hat{\Omega}^1_{O_{K_{\rm ur}}}\longrightarrow\hat{\Omega}^1_{O_{K_{\rm ur}}}$ is uniquely determined by the following properties:
a) $C(\mathrm{d}(\hat{O}_{K_{\rm ur}}))=0$;
b) if $f\in t\hat{O}_{K_{\rm ur}}$ then $C(f^p\,\mathrm{d}(t)/t)=f\,\mathrm{d}(t)/t$.
It can be shown that the definition of C does not depend on the choice of the uniformiser t, C is σ^{-1}-linear and $\mathrm{Ker}C=\mathrm{d}(\hat{O}_{K_{\rm ur}})$.

The following properties of admissible systems $f_{KK'}=\{f_{KK's}\}_{s\geqslant 0}$ follow directly from the above definition:

(1) the map $f_{KK'\infty}$ is uniquely determined by $f_{KK'{\rm ur}}$;

(2) if $K''=k((t''))\subset K(p)$ and $g_{K'K''}=\{g_{K'K''s}\}_{s\geqslant 0}$ is admissible then so is the composition $(fg)_{KK''}:=\{f_{KK's}g_{K'K''s}\}_{s\geqslant 0}$ and it holds $(fg)_{KK''\infty}=f_{KK'\infty}g_{K'K''\infty}$;

(3) $f_{KK'\infty}(\mathrm{d}\,\hat{O}_{K_{\rm ur}})\subset\mathrm{d}\,\hat{O}_{K'_{\rm ur}}$;

(4) for all $a,b\in\mathbb{Z}(p)$ and $m\in\mathbb{Z}_{\geqslant 0}$, there are unique $\alpha^{\infty}_{a,b,-m}(f_{KK'})\in k(p)$ such that if $n\geqslant 0$ then

$$f_{KK'\infty}\left(t^{ap^n}\frac{\mathrm{d}(t)}{t}\right)=\sum_{\substack{b\in\mathbb{Z}(p)\\0\leqslant m\leqslant n}}\sigma^n\alpha^{\infty}_{a,b,-m}(f_{KK'})t'^{bp^{n-m}}\frac{\mathrm{d}(t')}{t'};\tag{3.1}$$

(5) the above coefficients $\alpha^{\infty}_{a,b,-m}(f_{KK'})$ satisfy the following property: if $b/p^m<a$ then $\alpha^{\infty}_{a,b,-m}(f_{KK'})=0$.

Definition. With the above notation an admissible compatible system $f_{KK'}$ will be called special admissible if $f_{KK'{\rm ur}}(\mathcal{M}_{K\infty})\subset\mathcal{M}_{K'\infty}$.

Notice that the composition of special admissible systems is again special admissible.

3.4. Characterisation of special admissible systems. Let $f_{KK'}=\{f_{KK's}\}_{s\geqslant 0}$ be a compatible system. Then for any $s\geqslant 0$, the $k(p)$-linear morphism $f_{KK's}:\bar{\mathcal{M}}_{Ks}\longrightarrow\bar{\mathcal{M}}_{K's}$ is defined over $\mathbb{F}_p$, i.e. it comes from a $\mathbb{F}_p$-linear morphism $f_{KK's}:\mathcal{M}_{Ks}\longrightarrow\mathcal{M}_{K's}$. Therefore, in terms of the standard generators $D^{(s)}_{an}$ and $D'^{(s)}_{an}$ (which correspond to the uniformisers $t=t_K$ and, resp., $t'=t_{K'}$), we have for any $s\geqslant 0$ and $a\in\mathbb{Z}(p)$ that

$$f_{KK's}(D^{(s)}_{a0})=\sum_{\substack{b\in\mathbb{Z}(p)\\m\in\mathbb{Z}\,\mathrm{mod}\,N_s}}\alpha_{abm}(f_{KK's})D'^{(s)}_{bm},$$

where all $\alpha_{abm}(f_{KK's}) \in k_s \subset k(p)$. Notice that for all $n \in \mathbb{Z} \bmod N_s$, it holds

$$f_{KK's}(D_{an}^{(s)}) = \sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z} \bmod N_s}} \sigma^n \alpha_{abm}(f_{KK's}) D_{b,m+n}^{\prime(s)}.$$

Proposition 3.3. *Suppose $f_{KK'} = \{f_{KK's}\}_{s\geqslant 0}$ is a compatible system. Then it is special admissible if and only if for any $s \geqslant 0$, there are $v_s \in \mathbb{N}$ such that $v_s \to \infty$ if $s \to \infty$, and if $a, b < v_s$, $m \geqslant 0$ and $b/p^m < a$ then $\alpha_{a,b,-m \bmod N_s}(f_{KK's}) = 0$.*

Proof. Suppose $f_{KK'}$ is special admissible. Then $f_{KK'\mathrm{ur}}(\mathcal{M}_{K\infty}) \subset \mathcal{M}_{K'\infty}$ and for all $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z}$,

$$f_{KK'\mathrm{ur}}(D_{an}^{\infty}) = \sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z}}} \beta_{anbm} D_{b,n+m}^{\prime\infty}.$$

Here all coefficients $\beta_{anbm} \in k(p)$ and because $f_{KK'\mathrm{ur}}$ commutes with σ, there are $\gamma_{abm} \in k(p)$ such that $\beta_{anbm} = \sigma^n(\gamma_{abm})$. Therefore, if $a, b \in \mathbb{Z}(p)$, $m \in \mathbb{Z}$ and $\gamma_{abm} \neq 0$ then $m \leqslant 0$ and $\alpha_{abm}^{\infty}(f_{KK'}) = \gamma_{abm}$.

If $s \geqslant 0$, $a \in \mathbb{Z}(p)$,

$$f_{KK's}(D_{a0}^{(s)}) = \sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z} \bmod N_s}} \alpha_{a,b,-m}(f_{KK's}) D_{b,-m}^{\prime(s)}$$

and $b/p^{N_s} < a$ then for any $m \geqslant 0$, $\alpha_{a,b,-m \bmod N_s}(f_{KK's}) = \alpha_{a,b,-m}^{\infty}(f_{KK'})$. This implies that $\alpha_{a,b,-m \bmod N_s}(f_{KK's}) = 0$ if $a, b < p^{N_s}$ and $b/p^m < a$. Therefore, we can take $v_s = p^{N_s}$. This proves the "only if " part of the proposition.

Suppose now that $v_s \to \infty$ if $s \to \infty$ and for $a, b \in \mathbb{Z}(p)$, $m \geqslant 0$,

$$\alpha_{a,b,-m \bmod N_s}(f_{KK's}) = 0$$

if $a, b < v_s$ and $b/p^m < a$. If in addition $p^{N_s} > b$ then $\alpha_{a,b,-m \bmod N_s}(f_{KK's})$ does not depend on s and can be denoted by $\alpha_{a,b,-m}^{\infty}$. Clearly, $\alpha_{a,b,-m}^{\infty} = 0$ if $b/p^m < a$. Let $a \in \mathbb{Z}(p)$ and

$$d = f_{KK'\mathrm{ur}}(D_{a0}^{\infty}) - \sum_{\substack{b\in\mathbb{Z}(p)\\ m\geqslant 0}} \alpha_{a,b,-m}^{\infty} D_{b,-m}^{\prime\infty}.$$

Let $s \geqslant 0$ and let $d_s \in \bar{\mathcal{M}}_{Ks}$ be the image of d under the natural projection $\bar{\mathcal{M}}_{K\mathrm{ur}} \longrightarrow \bar{\mathcal{M}}_{Ks}$. If $s_1 \geqslant s$ then the corresponding projection $d_{s_1} \in \bar{\mathcal{M}}_{Ks_1}$ is a linear combination of $D_{bm}^{(s_1)}$ with $b > p^{N_{s_1}}$. Therefore, d_s also does not contain the terms $D_{bm}^{(s)}$ for which $b > p^{N_{s_1}}$. Because $\lim_{s_1\to\infty} N_{s_1} = \infty$, this implies that $d_s = 0$ for all $s \geqslant 0$ and, therefore, $d = 0$. So, $f_{KK'\mathrm{ur}}(\mathcal{M}_{K\infty}) \subset \mathcal{M}_{K'\infty}$.

Set $\alpha^{\infty}_{a,b,-m}(f_{KK'}) := \alpha^{\infty}_{a,b,-m}$ and define $f_{KK'\infty} : \hat\Omega^1_{O_{K_{\mathrm{ur}}}} \longrightarrow \hat\Omega^1_{O_{K'_{\mathrm{ur}}}}$ by formula (3.1). It is easy to see that $f_{KK'\infty}$ satisfies the requirements **A1-A3** from the definition of admissible system in Subsection 3.3. This proves the "if" part of our proposition.

□

Remark. Any special admissible $f_{KK'}$ can be defined as a $k(p)$-linear isomorphism $f_{KK'\mathrm{ur}} : \mathcal{M}_{K\infty} \longrightarrow \mathcal{M}_{K'\infty}$ such that

(1) $f_{KK'\mathrm{ur}}$ commutes with σ;

(2) if $a \in \mathbb{Z}(p)$ then

$$f_{KK'\mathrm{ur}}(D^{\infty}_{a0}) = \sum_{\substack{b\in\mathbb{Z}(p)\\ m\geqslant 0}} \alpha_{a,b,-m} D'^{\infty}_{b,-m}$$

where $\alpha_{a,b,-m} = 0$ if $b/p^m < a$.

3.5. Analytic compatible systems. Suppose $K, K' \subset K(p)$. Then the corresponding residue fields k and k' are subfields of the residue field $k(p) \subset \bar{\mathbb{F}}_{q_0}$. Therefore, if $K \simeq K'$ then $k = k'$ and we can introduce the set $\mathrm{Iso}^0(K, K')$ of field isomorphisms $\eta : K \longrightarrow K'$ such that $\eta|_k = \mathrm{id}$. Notice that any $\eta \in \mathrm{Iso}^0(K, K')$ induces a $k(p)$-linear map $\Omega^1(\eta) : \hat\Omega^1_{O_{K_{\mathrm{ur}}}} \longrightarrow \hat\Omega^1_{O_{K'_{\mathrm{ur}}}}$.

For all $s \geqslant 0$, any $\eta \in \mathrm{Iso}^0(K, K')$ can be naturally extended to $\eta_s \in \mathrm{Iso}^0(K_s, K'_s)$. Then $\eta^*_{KK'} = \{\eta^*_s\}_{s\geqslant 0}$ is a compatible system and $\eta_{KK'\infty} = \Omega^1(\eta)$. Propositions 2.4 and 3.3 imply that $\eta^*_{KK'}$ is a special admissible system.

Consider the opposite situation. Choose a uniformiser t_K in K and introduce $\mathrm{Fr}(t_K) \in \mathrm{Aut}(K_{\mathrm{ur}})$ such that $\mathrm{Fr}(t_K) : t_K \mapsto t_K$ and $\mathrm{Fr}(t_K)|_{k(p)} = \sigma$. Then for all $s \geqslant 0$, $\mathrm{Fr}(t_K)$ induces an automorphism of K_s which will be denoted by $\mathrm{Fr}(t_K)_s$. Then $\mathrm{Fr}(t_K)^* = \{\mathrm{Fr}(t_K)_s\}_{s\geqslant 0}$ is a compatible system, but this system is not admissible: the corresponding map $\mathrm{Fr}(t_K)_\infty$ coincides with the Cartier operator and, therefore, is not $k(p)$-linear.

More generally, consider a compatible system $\theta_{KK'} = \{\theta_{KK's}\}_{s\geqslant 0}$ where for all $s \geqslant 0$, $\theta_{KK's} = \theta^*_s$ and $\theta_s \in \mathrm{Iso}(K_s, K'_s)$. Then after choosing a uniformising element $t_{K'}$ in K' we have $\theta_s = \eta_s \mathrm{Fr}(t_{K'})^{n_s}$, for all $s \geqslant 0$, where $\eta_s \in \mathrm{Iso}^0(K_s, K'_s)$ and $n_{s+1} \equiv n_s \bmod N_s$. If $\bar n = \varprojlim_s n_s \in \varprojlim_s \mathbb{Z}/N_s\mathbb{Z}$ then $\theta_{KK'}$ is the composite of the special admissible system $\{\eta^*_s\}_{s\geqslant 0}$ and the system $\mathrm{Fr}(t_{K'})^{\bar n *}$ which is special admissible if and only if $\bar n = 0$. Therefore, $\theta_{KK'}$ is special admissible if and only if it comes from a compatible system of field isomorphisms $\eta_s \in \mathrm{Iso}^0(K_s, K'_s)$.

3.6. Locally analytic systems.

Definition. If $f_{KK'}$ is an admissible system, then $f_{KK'\mathrm{an}} := f_{KK'\infty}|_{\mathrm{d}(\hat{O}_{K_{\mathrm{ur}}})}$.

Remark. Notice the following similarity to the definition of f_{an} for $f \in \mathrm{Aut}\mathcal{M}$ from n.2.3. If $f_{KK} = \{f_{KKs}\}_{s\geqslant 0}$ is any admissible system then $g_{KK} := \{f_{KKs\mathrm{an}}\}_{s\geqslant 0}$ is also admissible and $f_{KK\mathrm{an}} = g_{KK\mathrm{an}}$.

Definition. An admissible system $f_{KK'} = \{f_{KK's}\}_{s\geqslant 0}$ will be called locally analytic if for any $s \geqslant 0$, there are $v_s \in \mathbb{N}$ and $\eta_s \in \mathrm{Iso}^0(K, K')$ such that $v_s \to +\infty$ as $s \to \infty$ and $f_{KK'\mathrm{an}} \equiv \mathrm{d}(\eta_s)\hat{\otimes}_k k(p) \,\mathrm{mod}\, t'^{v_s}$.

Proposition 3.4. *Suppose that $f_{KK'} = \{f_{KK's}\}_{s\geqslant 0}$ is special admissible and locally analytic. Then there is an $\eta \in \mathrm{Iso}^0(K, K')$ such that $f_{KK'\mathrm{an}} = \mathrm{d}(\eta)\hat{\otimes}_k k(p)$.*

Proof. If $s \geqslant 0$ and $a, b \in \mathbb{Z}(p)$ are such that $v_s/p^{N_0} < a, b < v_s$, then

$$\alpha^{\infty}_{ab0}(f_{KK'}) = \alpha_{ab0}(\eta^*_s) = \alpha_{ab0}(f_{KK's}) = \alpha_{ab0}(f_{KK'0}) \in k.$$

Therefore, by Proposition 2.7, all conjugates of η_s over K are congruent modulo $t'^{v_s(1-p^{-N_0})/\delta_p}$, and $\eta_s(t) \in k[[t']] \,\mathrm{mod}\, t'^{v_s(1-p^{-N_s})/\delta_p}$, where δ_p is 1 if $p \neq 2$ and $\delta_p = 2$ if $p = 2$. This implies that $\alpha_{ab0}(f_{KK's}) \in k$ if $a, b < v_s(1 - p^{-N_s})/\delta_p$.

If $b < p^{N_s}$ then $\alpha_{ab0}(f_{KK's}) = \alpha^{\infty}_{ab0}(f_{KK'})$. So, $\alpha^{\infty}_{ab0}(f_{KK'}) \in k$ if $b < c_s := \min\left\{p^{N_s}, v_s(1 - p^{-N_s})/\delta_p\right\}$. But $c_s \to \infty$ if $s \to \infty$ and, therefore, $\alpha^{\infty}_{ab0}(f_{KK'}) \in k$ for all $a, b \in \mathbb{Z}(p)$.

As we have already noticed, if $b < \min\{p^{N_s}, v_s\}$ then

$$\alpha_{ab0}(f_{KK's}) = \alpha_{ab0}(\eta^*_s) = \alpha^{\infty}_{ab0}(f_{KK'}).$$

Therefore, by Proposition 2.7 there exists $\varprojlim_s \eta_s := \eta \in \mathrm{Iso}^0(K, K')$ and $f_{KK'\mathrm{an}} = \mathrm{d}(\eta)\hat{\otimes}_k k(p)$.

The proposition is proved. □

3.7. Comparability of admissible systems. With the above notation suppose L, L' are finite field extensions of K, resp. K', in $K(p)$. Let $g_{LL'} = \{g_{LL's}\}_{s\geqslant 0}$ be a compatible family of continuous field isomorphisms $g_{LL's} : L_s \longrightarrow L'_s$. Then the natural embeddings $\Gamma_L(p) \subset \Gamma_K(p)$ and $\Gamma_{L'}(p) \subset \Gamma_{K'}(p)$ induce embeddings $\Gamma_{L_s}(p) \subset \Gamma_{K_s}(p)$ and $\Gamma_{L'_s}(p) \subset \Gamma_{K'_s}(p)$, for any $s \geqslant 0$.

Definition. With the above assumptions the systems $g_{LL'}$ and $f_{KK'}$ will be called comparable if, for all $s \geqslant 0$, there is the following commutative diagram

$$\begin{array}{ccc} \mathcal{M}_{Ls} & \xrightarrow{g_{LL's}} & \mathcal{M}_{L's} \\ \downarrow j_s & & \downarrow j'_s \\ \mathcal{M}_{Ks} & \xrightarrow{f_{KK's}} & \mathcal{M}_{K's} \end{array}$$

where the vertical arrows j_s and j'_s are induced by the embeddings $\Gamma_{L_s}(p) \subset \Gamma_{K_s}(p)$ and, resp., $\Gamma_{L'_s}(p) \subset \Gamma_{K'_s}(p)$.

If $g_{LL'}$ and $f_{KK'}$ are comparable then we have the following commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{M}}_{L\mathrm{ur}} & \xrightarrow{g_{LL'\mathrm{ur}}} & \bar{\mathcal{M}}_{L'\mathrm{ur}} \\ \downarrow j_{\mathrm{ur}} & & \downarrow j'_{\mathrm{ur}} \\ \bar{\mathcal{M}}_{K\mathrm{ur}} & \xrightarrow{f_{KK'\mathrm{ur}}} & \bar{\mathcal{M}}_{K'\mathrm{ur}} \end{array} \tag{3.2}$$

where $j_{\mathrm{ur}} := \varprojlim_s j_s \hat{\otimes}_{k_s} k(p)$ and $j'_{\mathrm{ur}} := \varprojlim_s j'_s \hat{\otimes}_{k_s} k(p)$. Notice that j_{ur} and j'_{ur} are epimorphic. Indeed, let U_{L_s}, U_{K_s} be principal units in L_s, resp. K_s. Then $\mathcal{M}_{L\mathrm{ur}} = \varprojlim_s U_{L_s}/U^p_{L_s}$ and $\mathcal{M}_{K\mathrm{ur}} = \varprojlim_s U_{K_s}/U^p_{K_s}$ contain as dense subsets the images of the groups of principal units $U_{L_{\mathrm{ur}}}$, resp. $U_{K_{\mathrm{ur}}}$, of the fields L_{ur}, resp. K_{ur}. By class field theory, j_{ur} is induced by the norm map $N = N_{L_{\mathrm{ur}}/K_{\mathrm{ur}}}$ from L^*_{ur} to K^*_{ur}. By [6], Ch 2, $N(U_{L_{\mathrm{ur}}})$ is dense in $U_{K_{\mathrm{ur}}}$ and, therefore, j_{ur} (together with j'_{ur}) is surjective.

Suppose L/K and L'/K' are Galois extensions. Denote their inertia subgroups by $I_{L/K}$ and $I_{L'/K'}$. Then we have identifications $I_{L/K} = \mathrm{Gal}(L_{\mathrm{ur}}/K_{\mathrm{ur}})$ and $I_{L'/K'} = \mathrm{Gal}(L'_{\mathrm{ur}}/K'_{\mathrm{ur}})$.

Consider the following condition:

C. *There is a group isomorphism $\kappa : I_{L/K} \longrightarrow I_{L'/K'}$ such that for any $\tau \in I_{L/K}$, $\tau^*_{LL\mathrm{ur}} g_{LL'\mathrm{ur}} = g_{LL'\mathrm{ur}} \kappa(\tau)^*_{L'L'\mathrm{ur}}$.*

Proposition 3.5. *Suppose $g_{LL'}$ and $f_{KK'}$ are comparable and $g_{LL'}$ satisfies the above condition* **C***. If $g_{LL'}$ is admissible then $f_{KK'}$ is also admissible.*

Proof. Because $g_{LL'}$ is admissible we have the following commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{M}}_{L\mathrm{ur}} & \xrightarrow{g_{LL'\mathrm{ur}}} & \bar{\mathcal{M}}_{L'\mathrm{ur}} \\ \Big\downarrow \pi_{L\mathrm{ur}} & & \Big\downarrow \pi_{L'\mathrm{ur}} \\ \hat{\Omega}^1_{O_{L_{\mathrm{ur}}}} & \xrightarrow{g_{LL'\infty}} & \hat{\Omega}^1_{O_{L'_{\mathrm{ur}}}} \end{array} \tag{3.3}$$

If $\tau \in I_{L/K} \subset \mathrm{Aut}^0(L_{\mathrm{ur}})$ then it follows from the definition of $\pi_{L_{\mathrm{ur}}}$ that

$$\tau^* \pi_{L\mathrm{ur}} = \pi_{L\mathrm{ur}} \Omega(\tau). \tag{3.4}$$

This means that $\pi_{L\mathrm{ur}}$ transforms the natural action of $I_{L/K}$ on $\bar{\mathcal{M}}_{L\mathrm{ur}}$ into the natural action of $I_{L/K}$ on $\hat{\Omega}^1_{O_{L_{\mathrm{ur}}}}$. Because j_{ur} is induced by the norm map of the field extension $L_{\mathrm{ur}}/K_{\mathrm{ur}}$, this gives us the following commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{M}}_{L\mathrm{ur}} & \xrightarrow{\pi_{L\mathrm{ur}}} & \hat{\Omega}^1_{O_{L_{\mathrm{ur}}}} \\ \Big\downarrow j_{\mathrm{ur}} & & \Big\downarrow \mathrm{Tr} \\ \bar{\mathcal{M}}_{K\mathrm{ur}} & \xrightarrow{\pi_{K\mathrm{ur}}} & \hat{\Omega}^1_{O_{K_{\mathrm{ur}}}} \end{array} \tag{3.5}$$

where Tr is induced by the trace of the extension $L_{\mathrm{ur}}/K_{\mathrm{ur}}$. Similarly, we have the commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{M}}_{L'\mathrm{ur}} & \xrightarrow{\pi_{L'\mathrm{ur}}} & \hat{\Omega}^1_{O_{L'_{\mathrm{ur}}}} \\ \Big\downarrow j'_{\mathrm{ur}} & & \Big\downarrow \mathrm{Tr}' \\ \bar{\mathcal{M}}_{K'\mathrm{ur}} & \xrightarrow{\pi_{K'\mathrm{ur}}} & \hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}} \end{array} \tag{3.6}$$

We have already seen that $\pi_{L\mathrm{ur}}$, $\pi_{L'\mathrm{ur}}$, j_{ur} and j'_{ur} are surjective. The traces Tr and Tr$'$ are also surjective. Indeed, suppose t_L, resp. t_K, are uniformising elements for L, resp. K. Then

$$\hat{\Omega}^1_{O_{L_{\mathrm{ur}}}} = \{f\,\mathrm{d}(t_L) \mid f \in \hat{O}_{L_{\mathrm{ur}}}\} = \{g\,\mathrm{d}(t_K) \mid g \in \mathcal{D}(L/K)^{-1}\hat{O}_{L_{\mathrm{ur}}}\},$$

where $\mathcal{D}(L/K)$ is the different of the extension L/K. It remains to notice that $\mathrm{Tr}(\mathcal{D}(L/K)^{-1}\hat{O}_{L_{\mathrm{ur}}}) = \hat{O}_{K_{\mathrm{ur}}}$.

Because $g_{LL'}$ and $f_{KK'}$ are comparable, we have the following commutative diagram

$$
\begin{array}{ccc}
\bar{\mathcal{M}}_{L\mathrm{ur}} & \xrightarrow{g_{LL'\mathrm{ur}}} & \bar{\mathcal{M}}_{L'\mathrm{ur}} \\
\big\downarrow j_{\mathrm{ur}} & & \big\downarrow j'_{\mathrm{ur}} \\
\bar{\mathcal{M}}_{K\mathrm{ur}} & \xrightarrow{f_{KK'\mathrm{ur}}} & \bar{\mathcal{M}}_{K'\mathrm{ur}}
\end{array}
\tag{3.7}
$$

Suppose $\omega_K \in \hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$. As it has been proved there is an $\omega_L \in \hat{\Omega}^1_{O_{L_{\mathrm{ur}}}}$ such that

$$\mathrm{Tr}(\omega_L) = \sum_{\tau \in I_{L/K}} \Omega(\tau)(\omega_L) = \omega_K.$$

Then

$$
\begin{aligned}
g_{LL'\infty}(\omega_K) &= \sum_{\tau \in I_{L/K}} g_{LL'\infty}(\Omega(\tau)(\omega_L)) \\
&= \sum_{\tau' \in I_{L'/K'}} \Omega(\tau')(g_{LL'\infty}(\omega_L)) = \mathrm{Tr}'(g_{LL'\infty}(\omega_L)) \in \hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}
\end{aligned}
\tag{3.8}
$$

because $\Omega(\tau)g_{LL'\infty} = g_{LL'\infty}\Omega(\kappa(\tau))$, for any $\tau \in I_{L/K}$. This equality is implied by the following computations (we use the commutative diagrams (3.3), (3.4) and condition **C**)

$$
\begin{aligned}
\pi_{L\mathrm{ur}}\Omega(\tau)g_{LL'\infty} &= \tau^*\pi_{L\mathrm{ur}}g_{LL'\infty} = \tau^* g_{LL'\mathrm{ur}}\pi_{L'\mathrm{ur}} \\
&= g_{LL'\mathrm{ur}}\kappa(\tau)^*\pi_{L'\mathrm{ur}} = g_{LL'\mathrm{ur}}\pi_{L'\mathrm{ur}}\Omega(\kappa(\tau)) \\
&= \pi_{L\mathrm{ur}}g_{LL'\infty}\Omega(\kappa(\tau)),
\end{aligned}
$$

because $\pi_{L_{\mathrm{ur}}}$ is surjective.

Let $f_{KK'\infty}$ be the restriction of $g_{LL'\infty}$ on $\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}$. Then formula (3.8) implies that $f_{KK'\infty}(\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}}) \subset \hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}$ and we have the following commutative diagram

$$
\begin{array}{ccc}
\hat{\Omega}^1_{O_{L_{\mathrm{ur}}}} & \xrightarrow{g_{LL'\infty}} & \hat{\Omega}^1_{O_{L'_{\mathrm{ur}}}} \\
\big\downarrow \mathrm{Tr} & & \big\downarrow \mathrm{Tr}' \\
\hat{\Omega}^1_{O_{K_{\mathrm{ur}}}} & \xrightarrow{f_{KK'\infty}} & \hat{\Omega}^1_{O_{K'_{\mathrm{ur}}}}
\end{array}
\tag{3.9}
$$

We now verify that $f_{KK'\infty}$ satisfies the requirements **A1-A3** from n.3.3. Property **A1** means that we have the following commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{M}}_{K_{\rm ur}} & \xrightarrow{f_{KK'{\rm ur}}} & \bar{\mathcal{M}}_{K'_{\rm ur}} \\ \downarrow \pi_{K_{\rm ur}} & & \downarrow \pi_{K'_{\rm ur}} \\ \hat\Omega^1_{O_{K_{\rm ur}}} & \xrightarrow{f_{KK'\infty}} & \hat\Omega^1_{O_{K'_{\rm ur}}} \end{array}$$

Its commutativity is implied by the following computations (we use commutative diagrams (3.2), (3.5), (3.3) and (3.9))

$$\begin{aligned} j_{\rm ur} f_{KK'{\rm ur}} \pi_{K'{\rm ur}} &= g_{LL'{\rm ur}} j'_{\rm ur} \pi_{K'{\rm ur}} = g_{LL'{\rm ur}} \pi_{L'{\rm ur}} {\rm Tr}' \\ &= \pi_{L{\rm ur}} g_{LL'\infty} {\rm Tr}' = \pi_{L{\rm ur}} {\rm Tr} f_{KK'\infty} = j_{\rm ur} \pi_{K{\rm ur}} f_{KK'\infty} \end{aligned}$$

because $j_{\rm ur}$ is surjective.

Let C_K, $C_{K'}$, C_L and $C_{L'}$ be the Cartier operators on, resp., $\hat\Omega^1_{O_{K_{\rm ur}}}$, $\hat\Omega^1_{O_{K'_{\rm ur}}}$, $\hat\Omega^1_{O_{L_{\rm ur}}}$ and $\hat\Omega^1_{O_{L'_{\rm ur}}}$. Clearly, $C_L{\rm Tr} = {\rm Tr}C_K$ and $C_{L'}{\rm Tr}' = {\rm Tr}'C_{K'}$. Then it follows from the commutative diagram (3.9) and property **A2** for $g_{LL'\infty}$ that

$$\begin{aligned} {\rm Tr} C_K f_{KK'\infty} &= C_L {\rm Tr} f_{KK'\infty} = C_L g_{LL'\infty} {\rm Tr} \\ &= g_{LL'\infty} C_{L'} {\rm Tr} = g_{LL'\infty} {\rm Tr} C_{K'} = {\rm Tr} f_{KK'\infty} C_{K'}. \end{aligned}$$

Property **A2** for $f_{KK'\infty}$ follows because Tr is surjective.

By condition **C**, the ramification indices e and e' of the extensions $L_{\rm ur}/K_{\rm ur}$ and $L'_{\rm ur}/K'_{\rm ur}$ are equal. Then we use the condition **A3** for $g_{LL'\infty}$ to deduce that for any $n \geqslant 0$,

$$g_{LL'\infty}(t_K^n \hat\Omega^1_{O_{L_{\rm ur}}}) = g_{LL'\infty}(t_L^{en} \hat\Omega^1_{O_{L_{\rm ur}}}) = t_L'^{e'n} \hat\Omega^1_{O_{L'_{\rm ur}}} = t_{K'}^n \hat\Omega^1_{O_{L'_{\rm ur}}}.$$

Therefore, it follows from the commutativity of diagram (3.9) that

$$\begin{aligned} t_{K'}^n \hat\Omega^1_{O_{K'_{\rm ur}}} &= t_{K'}^n {\rm Tr}'(\hat\Omega^1_{O_{L'_{\rm ur}}}) = {\rm Tr}'(g_{LL'\infty}(t_K^n \hat\Omega^1_{O_{L_{\rm ur}}})) \\ &= f_{KK'\infty}({\rm Tr}(t_K^n \hat\Omega^1_{O_{L_{\rm ur}}})) = f_{KK'\infty}(t_{K'}^n \hat\Omega^1_{O_{K_{\rm ur}}}). \end{aligned}$$

The proposition is proved. □

Remark. Using the embeddings of the Galois groups $\Gamma_{L_s}(p)$ and $\Gamma_{K_s}(p)$ into their Magnus's algebras from n.1.3, one can prove in addition that if $g_{LL'}$ is special then $f_{KK'}$ is also special. In other words, under condition **C**, $j_{\rm ur}(\mathcal{M}_{L\infty}) \subset \mathcal{M}_{K\infty}$.

Suppose $g_{LL'}$ and $f_{KK'}$ are comparable systems. Suppose also that $g_{LL'}$ and $f_{KK'}$ are special admissible, locally analytic and satisfy condition **C**. Then there are $\eta_{LL'} \in {\rm Iso}^0(L, L')$ and $\eta_{KK'} \in {\rm Iso}^0(K, K')$ such that $f_{KK'\infty}|_{{\rm d}\,\hat O_{K_{\rm ur}}} = {\rm d}(\eta_{KK'})\hat\otimes_k k(p)$ and $g_{LL'\infty}|_{{\rm d}\,\hat O_{L_{\rm ur}}} = {\rm d}(\eta_{LL'})\hat\otimes_{k_L} k_L(p)$.

Proposition 3.6. *With the above notation and assumptions,* $\eta_{LL'}|_K = \eta_{KK'}$.

Proof. Clearly, for any $\tau \in I_{L/K}$, condition **C** implies that $\tau^*_{LL\infty} g_{LL'\infty} = g_{LL'\infty}\kappa(\tau)^*_{L'L'\infty}$. Restricting this equality to $\mathrm{d}\,\hat{O}_{L_{\mathrm{ur}}}$, we obtain

$$\mathrm{d}(\tau)\,\mathrm{d}(\eta_{LL'}) = \mathrm{d}(\eta_{LL'})\,\mathrm{d}(\kappa(\tau)).$$

Then it follows from proposition 2.7 that $\tau\eta_{LL'} = \eta_{LL'}\kappa(\tau)$. Therefore, $\eta_{LL'}|_K$ induces a ring isomorphism from $\hat{O}_{K_{\mathrm{ur}}}$ onto $\hat{O}_{K'_{\mathrm{ur}}}$.

Suppose $a \in \mathrm{Tr}(\hat{O}_{L_{\mathrm{ur}}}) \subset \hat{O}_{K_{\mathrm{ur}}}$. If $a = \mathrm{Tr}(b)$ with $b \in \hat{O}_{L_{\mathrm{ur}}}$ then it follows from diagram (3.9) and condition **C** that

$$\mathrm{d}(\eta_{KK'}(a)) = \mathrm{Tr}'(\mathrm{d}(\eta_{LL'}(b))) = \sum_{\tau' \in I_{L'/K'}} \mathrm{d}(\tau')\,(\mathrm{d}(\eta_{LL'}(b)))$$

$$= \sum_{\tau \in I_{L/K}} \mathrm{d}(\eta_{LL'})(\mathrm{d}(\tau(b))) = \mathrm{d}\,\eta_{LL'}(\mathrm{d}\,a) = \mathrm{d}(\eta_{LL'}(a)).$$

Therefore, for a sufficiently large $M \in \mathbb{N}$, $\mathrm{d}\,(\eta_{LL'}|_K)$ and $\mathrm{d}\,\eta_{KK'}$ coincide on $t_K^M \hat{O}_{K_{\mathrm{ur}}}$. Then proposition 2.7 implies that $\eta_{LL'}|_K = \eta_{KK'}$.

The proposition is proved. □

4. Explicit description of the ramification ideals $\mathcal{A}^{(v)}$ mod J^3

We return to the notation from Section 1. In particular, $\mathcal{A}$ is the $\mathbb{Z}_p$-algebra from Subsection 1.2, $\mathcal{J}$ is its augmentation ideal, $\mathcal{A}_k = \mathcal{A}\otimes W(k)$, $\mathcal{J}_k = \mathcal{J}\otimes W(k)$, $\mathcal{A}_K = \mathcal{A}\otimes O(K)$, etc. are the corresponding extensions of scalars, $e \in \mathcal{A}_K$ is the element introduced in Subsection 1.3. We fix an $f \in \mathcal{A}_{K(p)}$ such that $\sigma f = fe$ and denote the embedding $\psi_f : \Gamma(p) \longrightarrow (1+\mathcal{J})^\times$ by ψ.

4.1. Ramification filtration on $\mathcal{A}$

For any $v \geqslant 0$, consider the ramification subgroup $\Gamma(p)^{(v)}$ of $\Gamma(p)$ in the upper numbering. Denote by $\mathcal{A}^{(v)}$ the minimal 2-sided closed ideal in $\mathcal{A}$ containing the elements $\psi(\tau)-1$, for all $\tau \in \Gamma(p)^{(v)}$. Then $\{\mathcal{A}^{(v)} \mid v \geqslant 0\}$ is a decreasing filtration by closed ideals of $\mathcal{A}$. In particular, if $\mathcal{A}^{(v)}_{CM} \bmod \mathcal{J}^n_{CM}$ are the projections of $\mathcal{A}^{(v)}$ to $\mathcal{A}_{CM} \bmod \mathcal{J}^n_{CM}$, for $C, M, n \in \mathbb{N}$, then $\mathcal{A}^{(v)} = \varprojlim_{C,M,n} \mathcal{A}^{(v)}_{CM} \bmod \mathcal{J}^n_{CM}$. Notice also that the ramification filtration $\{\Gamma(p)^{(v)}\}_{v\geqslant 0}$ is left-continuous, i.e. $\Gamma(p)^{(v_0)} = \bigcap_{v<v_0} \Gamma(p)^{(v)}$, for any $v_0 > 0$. This implies a corresponding analogous property for the filtration $\{\mathcal{A}^{(v)} \mid v \geqslant 0\}$ on each finite level, i.e. for any $C, M, n \in \mathbb{N}$, we have the following property.

Proposition 4.1. *For any $C, M, n \in \mathbb{N}$ and $v_0 > 0$, there is a $0 < \delta < v_0$ such that $\mathcal{A}_{CM}^{(v)} \operatorname{mod} \mathcal{J}_{CM}^n = \mathcal{A}_{CM}^{(v_0)} \operatorname{mod} \mathcal{J}_{CM}^n$, for any $v \in (v_0 - \delta, v_0)$.*

Proof. This follows directly from the definition of the ramification filtration and the fact that the field of definition of each projection $f_{CM} \operatorname{mod} \mathcal{J}_{CM}^n$ of f to $\mathcal{A}_{CMK(p)} \operatorname{mod} \mathcal{J}_{CMK(p)}^n$ is a finite extension of K, cf. Subsection 1.3. □

Notice also that the class field theory implies the following property.

Proposition 4.2. *If $v \geqslant 0$ and $\mathcal{A}_k^{(v)} := \mathcal{A}^{(v)} \otimes W(k)$ then $\mathcal{A}_k^{(v)} \operatorname{mod} \mathcal{J}_k^2$ is topologically generated by all elements $p^s D_{an}$, for $n \in \mathbb{Z} \operatorname{mod} N_0$, $a \in \mathbb{Z}(p)$, $s \geqslant 0$ and $p^s a \geqslant v$.*

4.2. The filtration $\mathcal{A}(v)$, $v \geqslant 0$. For any $\gamma \geqslant 0$, introduce $\mathcal{F}_\gamma \in \mathcal{A}_k$ as follows.

If $\gamma = 0$ let $\mathcal{F}_\gamma = D_0$.

If $\gamma > 0$ let $\mathcal{F}_\gamma =$

$$p^{v_\gamma} a_\gamma D_{a_\gamma v_\gamma} - \sum_{\substack{a_1, a_2 \in \mathbb{Z}(p) \\ n \geqslant 0 \\ p^n(a_1 + a_2) = \gamma}} p^n a_1 D_{a_1 n} D_{a_2 n} - \sum_{\substack{a_1, a_2 \in \mathbb{Z}(p) \\ n_1 \geqslant 0, n_2 < n_1 \\ p^{n_1} a_1 + p^{n_2} a_2 = \gamma}} p^{n_1} a_1 [D_{a_1 n_1}, D_{a_2 n_2}].$$

Here the first two terms appear only if $\gamma \in \mathbb{N}$, and the corresponding $v_\gamma \in \mathbb{Z}_{\geqslant 0}$ and $a_\gamma \in \mathbb{Z}(p)$ are uniquely determined from the equality $\gamma = p^{v_\gamma} a_\gamma$. If $\gamma \notin \mathbb{Z}$ then the above formula for $\mathcal{F}_\gamma$ contains only the last sum.

For any $v \geqslant 0$, let $\mathcal{A}(v)$ be the minimal closed ideal in $\mathcal{A}$ such that $\mathcal{F}_\gamma \in \mathcal{A}_k(v) := \mathcal{A}(v) \otimes W(k)$, for all $\gamma \geqslant v$. Equivalently, $\mathcal{A}_k(v)$ is the minimal σ-invariant closed ideal of $\mathcal{A}_k$, which contains all $\mathcal{F}_\gamma$ with $\gamma \geqslant v$.

Remark. a) For any $v \geqslant 0$, $\mathcal{A}^{(v)} \operatorname{mod} \mathcal{J}^2 = \mathcal{A}(v) \operatorname{mod} \mathcal{J}^2$.

b) The filtration $\{\mathcal{A}(v) \mid v \geqslant 0\}$ is left-continuous.

c) If $C, M \in \mathbb{N}$ and $\mathcal{A}_{CM}(v) \operatorname{mod} \mathcal{J}_{CM}^n$ is the image of $\mathcal{A}(v)$ in $\mathcal{A}_{CM} \operatorname{mod} \mathcal{J}_{CM}^n$, then $\mathcal{A}(v) \operatorname{mod} \mathcal{J}^n = \varprojlim_{C,M} \mathcal{A}_{CM}(v) \operatorname{mod} \mathcal{J}_{CM}^n$.

If $\gamma \geqslant v_0 \geqslant 0$, denote by $\tilde{\mathcal{F}}_\gamma(v_0)$ the elements in $\mathcal{A}_k$ given by the same expressions as $\mathcal{F}_\gamma$ but with the additional restriction $p^{n_1} a_1, p^{n_1} a_2 < v_0$ for all degree 2 terms $p^{n_1} a_1 D_{a_1 n_1} D_{a_2 n_2}$ or $p^{n_1} a_1 [D_{a_1 n_1}, D_{a_2, n_2}]$. Clearly, we have the following property.

Proposition 4.3. a) *$\mathcal{A}(v_0)$ operatornamemod$\mathcal{J}^3$ is the minimal ideal of $\mathcal{A}$ such that $\mathcal{A}_k(v_0)$ is generated by all elements $\tilde{\mathcal{F}}_\gamma(v_0)$ with $\gamma \geqslant v_0$.*

b) *If $\gamma \geqslant 2v_0$, then $\tilde{\mathcal{F}}_\gamma(v_0) = \gamma D_{a_\gamma v_\gamma}$.*

The following theorem is the main technical result about the structure of the ramification filtration that we need in this paper.

Theorem B. *For any* $v \geqslant 0$, $\mathcal{A}^{(v)} \operatorname{mod} \mathcal{J}^3 = \mathcal{A}(v) \operatorname{mod} \mathcal{J}^3$.

This theorem gives an explicit description of the ramification filtration $\{\mathcal{A}^{(v)}\}_{v\geqslant 0}$ on the level of p-extensions of nilpotent class 2. (On the level of abelian p-extensions such a description is given by the above Remark a).) Theorem B can also be stated in the following equivalent form, where we use the index $M+1$ instead of M to simplify the notation in its proof below.

Theorem B'. *Suppose* $C \in \mathbb{N}$, $M \in \mathbb{Z}_{\geqslant 0}$ *and* $v_0 > 0$. *If, for all* $v > v_0$,

$$\mathcal{A}^{(v)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(v) \operatorname{mod} \mathcal{J}^3_{C,M+1},$$

then

$$\mathcal{A}^{(v_0)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(v_0) \operatorname{mod} \mathcal{J}^3_{C,M+1}.$$

Clearly, Theorem B' follows from theorem B.

Conversely, notice first that, for a given $C \in \mathbb{N}$, $M \geqslant 0$ and $v \gg 0$,

$$\mathcal{A}^{(v)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(v) \operatorname{mod} \mathcal{J}^3_{C,M+1} = 0.$$

Indeed, this is obvious for the ideals $\mathcal{A}_{C,M}(v)$, because they are generated by the elements obtained from the above elements $\tilde{\mathcal{F}}_\gamma(v)$ by adding the restrictions $a_1, a_2, a_\gamma < C$ and $n_1, n_2, v_\gamma \leqslant M$. But then, for $\gamma \geqslant 2p^M C$, the conditions $p^{n_1}a_1 + p^{n_2}a_2 = \gamma$ (where $n_2 \leqslant n_1$) and $p^{v_\gamma}a_\gamma = \gamma$ are never satisfied. For the filtration $\{\mathcal{A}^{(v)}\}_{v\geqslant 0}$, we notice, as earlier, that the field of definition $K_{C,M+1,3}(f)$ of the image of f in $\mathcal{A}_{C,M+1,K(p)} \operatorname{mod} \mathcal{J}^3_{C,M+1,K(p)}$ is of finite degree over the basic field K. Therefore, for $v \gg 0$, the ramification subgroup $\Gamma(p)^{(v)}$ acts trivially on $K_{C,M+1,3}(f)$ and $\mathcal{A}^{(v)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = 0$.

Now we can apply descending transfinite induction on $v \geqslant 0$. Let

$$S_{C,M+1} = \{v \geqslant 0 \mid \mathcal{A}^{(v)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(v) \operatorname{mod} \mathcal{J}^3_{C,M+1}\}.$$

Then $S_{C,M+1} \neq \emptyset$. Let $v_0 = \inf S_{C,M+1}$.

If $v_0 > 0$ then $\mathcal{A}^{(v_0)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{CM}(v_0) \operatorname{mod} \mathcal{J}^3_{C,M+1}$ by Theorem B'. By the left-continuity property of both filtrations, there is a $\delta \in (0, v_0)$ such that $\mathcal{A}^{(v)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(v) \operatorname{mod} \mathcal{J}^3_{C,M+1}$ whenever $v \in (v_0 - \delta, v_0)$. So, $v_0 = \inf S_{C,M+1} \leqslant v_0 - \delta$. This is a contradiction, hence $v_0 = 0$. In this case we have $\mathcal{A}^{(0)}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1} \operatorname{mod} \mathcal{J}^3_{C,M+1} = \mathcal{A}_{C,M+1}(0) \operatorname{mod} \mathcal{J}^3_{C,M+1}$. This implies that $S_{C,M+1} = \mathbb{R}_{\geqslant 0}$, and Theorem B is deduced from Theorem B'.

The rest of this section is concerned with a proof of Theorem B'.

4.3. Auxiliary results.

4.3.1. ***The field*** $\boldsymbol{K(N^*, r^*)}$**.** Suppose $N^* \in \mathbb{N}$, $q = p^{N^*}$ and $r^* = m^*/(q-1)$, where $m^* \in \mathbb{Z}(p)$. Then there is a field $K_1 := K(N^*, r^*) \subset K_{\mathrm{sep}}$ such that

a) $[K_1 : K] = q$;

b) the Herbrand function $\varphi_{K_1/K}(x)$ has only one corner point (r^*, r^*);

c) $K_1 = k((t_{K_1}))$, where $t_{K_1}^q E(-1, t_{K_1}^{m^*}) = t_K$ and E is the generalised Artin-Hasse exponential introduced in n.1.4.

The field $K(N^*, r^*)$ appears as a subfield of $K(U)$, where $U^q - U = u^{-m^*}$ and $u^{q-1} = t_K$. It is of degree q over K. Its construction is explained in all detail in [2].

4.3.2. ***Relation between liftings of*** $\boldsymbol{K}$ ***and*** $\boldsymbol{K_1}$ ***modulo*** $\boldsymbol{p^{M+1}}$***,*** $\boldsymbol{M \geqslant 0}$**.** Recall that we use the uniformiser t_K in K to construct the liftings modulo p^{M+1} of K, $O_{M+1}(K) = W_{M+1}(k)((t))$ and of $K(p)$, $O_{M+1}(K(p))$, where $t = t_{K,M+1}$. We use the uniformiser t_{K_1} from above n.4.3.1 c) to construct analogous liftings for K_1, $O'_{M+1}(K_1) = W_{M+1}(k)((t_1))$ and for $K_1(p) \supset K(p)$, $O'_{M+1}(K_1(p))$. (Here $t_1 = t_{K_1,M+1}$ is the Teichmüller representative of t_{K_1} in $W_{M+1}(K_1(p))$.)

Note that, with the above notation the field embedding $K \subset K_1$ does not induce an embedding $O_{M+1}(K) \subset O'_{M+1}(K_1)$ for $M \geqslant 1$, because the Teichmüller representative $t_1 = t_{K_1,M+1} = [t_{K_1}]$ cannot be expressed in terms of the Teichmüller representative $t = t_{K,M+1} = [t_K]$. This difficulty can be overcome as follows. Take $t_K^{p^M}$ as a uniformising element for $\sigma^M K$ and consider the corresponding liftings modulo p^{M+1}, $O_{M+1}(\sigma^M K) = W_{M+1}(k)((t^{p^M}))$ and $O_{M+1}(\sigma^M K(p)) \subset O_{M+1}(K(p))$. From the definition of liftings it follows that

$$O_{M+1}(\sigma^M K) \subset W_{M+1}(\sigma^M K) \subset W_{M+1}(\sigma^M K_1) \subset O'_{M+1}(K_1) \subset W_{M+1}(K_1),$$

$$O_{M+1}(\sigma^M K(p)) \subset W_{M+1}(\sigma^M K(p)) \subset W_{M+1}(\sigma^M K_1(p)) \subset O'_{M+1}(K_1(p)) \subset W_{M+1}(K_1(p)).$$

Lemma 4.4. *With respect to the above embedding* $O_{M+1}(\sigma^M K) \subset O'_{M+1}(K_1)$ *we have*

$$t^{p^M} = t_1^{qp^M} E(-1, t_1^{m^*})^{p^M}.$$

Proof. If V is the Verschiebung morphism on $W_{M+1}(K_1)$ then property c) from n.4.3.1 is equivalent to the relation

$$t \equiv t_1^{qp^M} E(-1, t_1^{m^*}) \operatorname{mod} VW_{M+1}(K_1).$$

Then, for any $s \geqslant 0$, we have

$$t^{p^s} \equiv t_1^{qp^s} E(-1, t_1^{m^*})^{p^s} \bmod V^{s+1} W_{M+1}(K_1).$$

(Using that for any $w_1, w_2 \in W_M(K_1)$, $(Vw_1)(Vw_2) = V^2(F(w_1w_2))$ and $pV(w_1) = V^2(Fw_1)$.) For $s = M$ we obtain the statement of the lemma. □

4.3.3. *A criterion.* Consider $\sigma^M e = 1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-ap^M} D_{a,M} \in \mathcal{A} \otimes O(\sigma^M K)$, where $O(\sigma^M K) = \varprojlim_n O_n(\sigma^M K)$. Then $\sigma^M f \in \mathcal{A} \otimes O(\sigma^M K(p))$ satisfies the relation $\sigma(\sigma^M f) = (\sigma^M f)(\sigma^M e)$ and induces the same morphism $\psi : \Gamma(p) \longrightarrow \mathcal{A}$ as f. Indeed, for any $\tau \in \Gamma(p)$,

$$\tau(\sigma^M f)(\sigma^M f)^{-1} = \sigma^M(\tau(f)f^{-1}) = \sigma^M(\psi(\tau)) = \psi(\tau)$$

because σ acts trivially on $\mathcal{A}$.

This means that we can still study the structure of the ramification filtration $\{\mathcal{A}^{(v)} \bmod p^{M+1}\}_{v \geqslant 0}$ by working inside the lifting $O'_{M+1}(K_1(p)) \supset O_{M+1}(\sigma^M K(p))$ associated with our auxiliary field K_1 and its uniformiser t_{K_1}.

Set $\mathcal{B} = \mathcal{A}_{C,M+1} \bmod \mathcal{J}^3_{C,M+1}$ and for any rational number $v \geqslant 0$, $\mathcal{B}^{(v)} = \mathcal{A}^{(v)}_{C,M+1} \bmod \mathcal{J}_{C,M+1}$. We shall also use the notation $\mathcal{B}_k = \mathcal{B} \otimes W_{M+1}(k)$, $\mathcal{B}_{K_1} = \mathcal{B} \otimes O'_{M+1}(K_1)$, and $\mathcal{B}_{K_1(p)} = \mathcal{B} \otimes O'_{M+1}(K_1(p))$. Denote again by $\mathcal{J}$ the augmentation ideal in $\mathcal{B}$. Its extensions of scalars will be denoted similarly by $\mathcal{J}_k, \mathcal{J}_{K_1}$ and $\mathcal{J}_{K_1(p)}$.

Consider an abstract continuous field isomorphism $\alpha : K \longrightarrow K_1$, which is the identity on the residue fields and sends t_K to t_{K_1}. Consider its extension to the field isomorphism $\hat{\alpha} : K(p) \longrightarrow K_1(p)$. Then we have an induced isomorphism of liftings $\hat{\alpha} : O_{M+1}(K(p)) \longrightarrow O'_{M+1}(K_1(p))$. Use it to define the morphism

$$\mathrm{id} \otimes \hat{\alpha} : \mathcal{A}_{C,M+1,K(p)} \longrightarrow \mathcal{B}_{K_1(p)}$$

and set $f_1 := (\mathrm{id} \otimes \hat{\alpha})(f) \in \mathcal{B}_{K_1(p)}$. Then $\sigma(f_1) = f_1 e_1$, where $e_1 = (\mathrm{id} \otimes \hat{\alpha})(e) = 1 + \sum_{a \in \mathbb{Z}^0(p)} t_1^{-a} D_{a0}$.

If $N^* \equiv 0 \bmod N_0$, then $\sigma^{M+N^*}(D_{a0}) = \sigma^M(D_{a0}) = D_{aM}$ and we can relate the elements $\sigma^M e = 1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-ap^M} D_{a,M}$ and $\sigma^{M+N^*} e_1 = 1 + \sum_{a \in \mathbb{Z}^0(p)} t_1^{-ap^M q} D_{a,M}$ by the use of the relation between t and t_1 from lemma 4.4. So, it will be natural to compare the elements $\sigma^M f$ and $\sigma^{M+N^*} f_1$ in $\mathcal{B}_{K_1(p)}$ by introducing $X \in \mathcal{B}_{K_1(p)}$ such that $(\sigma^M f)(1 + X) = \sigma^{M+N^*} f_1$. This element will be used for the characterisation of the ideal $\mathcal{B}^{(v_0)}$ in proposition 4.5 below.

Notice first, that $\mathcal{B}^{(v_0)}$ is the minimal 2-sided ideal in $\mathcal{B}$ such that the field of definition of $f \bmod \mathcal{B}^{(v_0)}_{K_1(p)}$ is invariant under the action of the group

$\Gamma(p)^{(v_0)}$. In other words, if I is a 2-sided ideal in $\mathcal{B}$ and $K(f,I)$ is the field of definition of $f \bmod I_{K_1(p)}$, then I contains $\mathcal{B}^{(v_0)}$ if and only if the largest upper ramification number $v(K(f,I)/K)$ (= the 2nd coordinate of the last vertex of the graph of the Herbrand function $\varphi_{K(f,I)/K}$) is less than v_0.

With the above notation we have the following criterion.

Proposition 4.5. *Suppose $r^* = v(K_1/K) < v_0$. Then $\mathcal{B}^{(v_0)}$ is the minimal element in the set of all 2-sided ideals I such that if $K_1(X,I)$ is the field of definition of $X \bmod I_{K_1(p)}$ over K_1 then its largest upper ramification number satisfies $v(K_1(X,I)/K_1) < qv_0 - r^*(q-1)$.*

Proof. We must prove that for any 2-sided ideal I in $\mathcal{B}$,

$$v := v(K(f,I)/K) < v_0 \quad \Leftrightarrow \quad v_1(X) := v(K_1(X,I)/K_1) < qv_0 - r^*(q-1).$$

The following proof is similar to the proof of the corresponding statement from [1, 2].

Suppose $v < v_0$. The existence of the field isomorphism $\hat{\alpha}$ implies that $v(K_1(f_1,I)/K_1) = v$. Then

$$v_1 := v(K_1(f_1,I)/K) = \max\{r^*, \varphi_{K_1/K}(v)\} \tag{4.1}$$

Indeed, it is sufficient to look at the maximal vertex of the Herbrand function for the extension $K_1(f_1,I)/K$ and to use the composition property for the corresponding Herbrand functions $\varphi_{K_1(f_1,I)/K}(x) = \varphi_{K_1/K}(\varphi_{K_1(f_1,I)/K_1}(x))$. This implies that $v_1 = r^*$ if $r^* \geqslant v$ and $v_1 < v$ if $v > r^*$, where we have used that $\varphi_{K_1/K}(v) = r^* + (v - r^*)/q < v$ if $v > r^*$. Therefore, the largest upper ramification number of the composite $K(f,I)$ and $K_1(f_1,I)$ over K is $\max\{r^*, v\} < v_0$. Clearly, $K_1(X,I)$ is contained in this composite and, therefore, $v(X) := v(K_1(X,I)/K) < v_0$. Similarly to formula (4.1) we obtain that $v(X) = \max\{r^*, \varphi_{K_1/K}(v_1(X))\}$. Therefore, $\varphi_{K_1/K}(v_1(X)) < v_0$ and $v_1(X) < qv_0 - r^*(q-1)$.

Conversely, assume that $v_1(X) < qv_0 - r^*(q-1)$. Then

$$v(X) = \max\{r^*, \varphi_{K_1/K}(v_1(X))\} < v_0.$$

Suppose $v = v(K(f,I)/K) \geqslant v_0$. As earlier, the existence of $\hat{\alpha}$ implies that $v(K_1(f_1,I)/K_1) = v$ and similarly to (4.1) we have

$$v(K_1(f_1,I)/K) = \max\{r^*, \varphi_{K_1/K}(v)\} = \varphi_{K_1/K}(v) < v.$$

Therefore, the largest upper ramification number of the composite of $K_1(X,I)$ and $K_1(f_1,I)$ over K equals

$$\max\{v(K_1(X,I)/K), v(K_1(f_1,I)/K)\} = \max\{v(X), \varphi_{K_1/K}(v)\}.$$

Because $K(f,I)$ is contained in this composite, we have

$$v \leqslant \max\{v(X), \varphi_{K_1/K}(v)\}.$$

But $v \geqslant v_0 > v(X)$ and $v > \varphi_{K_1/K}(v)$. This contradiction proves the proposition. . $\square$

4.3.4. ***Choosing N^* and r^*.*** In order to apply the criterion from Proposition 4.5 we shall use the special choice of $K_1 = K(N^*, r^*)$, where $N^* \in \mathbb{N}$ and $r^* < v_0$ are specified as follows.

Introduce $\delta_1 := \min\{v_0 - p^s a \mid p^s a < v_0, a \leqslant C, a \in \mathbb{Z}^0(p)\}$, and $\delta_2 :=$

$$\min\{v_0 - (p^{s_1}a_1 + p^{s_2}a_2)| \\ p^{s_1}a_1 + p^{s_2}a_2 < v_0, a_1, a_2 \leqslant C, a_1, a_2 \in \mathbb{Z}^0(p), s_1, s_2 \in \mathbb{Z}\}.$$

One can see that for a sufficiently large natural number $N^* \equiv 0 \bmod N_0$, there exists $r^* = m^*/(q-1) < v_0$ with $q = p^{N^*}$ and $m^* \in \mathbb{Z}(p)$ such that

a) $-(v_0 - \delta_1)q + r^*(q-1) > Cp^M$;

b) $-(v_0 - \delta_2)q + r^*(q-1) > 0$;

c) $v_0 q < 2r^*(q-1)$.

So, we may assume that $K_1 = K(N^*, r^*)$ where $N^* \equiv 0 \bmod N_0$ and the above inequalities a)-c) hold.

4.4. A recurrence formula for X. Set $\Theta^* = t_1^{r^*(q-1)}$. Then

$$\omega = \sigma^M e - \sigma^{M+N^*} e_1 = \sum_{a \in \mathbb{Z}^0(p)} t_1^{-ap^M q}(E(a, \Theta^*)^{p^M} - 1)D_{aM} \in \mathcal{J}_{K_1}.$$

The relation $1 + X = (\sigma^M f)^{-1}(\sigma^{M+N^*} f_1)$ implies that

$$1 + \sigma X = (\sigma^M e)^{-1}(1 + X)(\sigma^{M+N^*} e_1)$$

and

$$X - \sigma X = \omega + (\sigma^M e - 1)\sigma X - X(\sigma^{M+N^*} e_1 - 1). \tag{4.2}$$

If $\bar{X} := X \bmod \mathcal{J}^2_{K_1(p)}$, then the above relation (4.2) gives $\bar{X} - \sigma\bar{X} = \omega \bmod \mathcal{J}^2_{K_1(p)}$. We shall use this relation in Subsection 4.5 below to study $\bar{X}$. Now (4.2) can be rewritten as

$$X - \sigma X = \omega - \omega(\sigma^{M+N^*} e_1 - 1) - [\sigma\bar{X}, \sigma^{M+N^*} e_1 - 1] + \omega\sigma(\bar{X}), \tag{4.3}$$

using that $X \equiv \omega + \sigma X \bmod \mathcal{J}^2_{K_1(p)}$. We shall use this relation in nn.4.6-4.7 below to study the field of definition of X.

4.5. The study of $\bar{X}$. For $0 \leqslant r \leqslant M$ and $b \in \mathbb{Z}_p$, introduce $\mathcal{E}_r(b,T) \in \mathbb{Z}_p[[T]]$ as follows:

$\mathcal{E}_0(b,T) = E(b,T) - 1$, where $E(b,T)$ is the generalisation of the Artin-Hasse exponential from n.1.4;

$\mathcal{E}_1(b,T) = E(b,T)^p - E(b,T^p) = (\exp(pbT) - 1)E(b,T^p)$,

....

$\mathcal{E}_M(b,T) = E(b,T)^{p^M} - E(b,T^p)^{p^{M-1}} = (\exp(p^M bT) - 1)E(b,T^p)^{p^{M-1}}$.

Notice the following simple properties:

(1) $E(b,T)^{p^M} - 1 = \mathcal{E}_0(b,T^{p^M}) + \mathcal{E}_1(b,T^{p^{M-1}}) + \cdots + \mathcal{E}_M(b,T)$;

(2) $\mathcal{E}_r(b,T) = p^r T + p^r T^2 g_r(T)$, where $0 \leqslant r \leqslant M$ and $g_r \in \mathbb{Z}_p[[T]]$.

Consider the decomposition $\omega = \sum_{r+s=M} \sigma^r \omega_s$ (cf. Subsection 4.4 for the definition of ω), where

$$\omega_s := \sum_{a \in \mathbb{Z}^0(p)} t_1^{-ap^s q} \mathcal{E}_s(a, \Theta^*) D_{as},$$

for $0 \leqslant s \leqslant M$. Note that $p^s D_{as} \in \mathcal{B}_k^{(v_0)} \operatorname{mod} \mathcal{J}_k^2$, whenever $p^s a \geqslant v_0$, cf. proposition 4.2. Also, if $p^s a < v_0$ then $-ap^s q + r^*(q-1) > Cp^M$, cf. Subsubsection 4.3.4, and we have $t_1^{-ap^s q} \mathcal{E}_s(a, \Theta^*) \in t_1^{Cp^M} \mathrm{m}_1$, where $\mathrm{m}_1 := t_1 W_M(k)[[t_1]]$.

So, for $0 \leqslant s \leqslant M$,

$$\omega_s \in \mathcal{B}_{K_1}^{(v_0)} + t_1^{Cp^M} \mathcal{J}_{\mathrm{m}_1} + \mathcal{J}_{K_1}^2, \tag{4.4}$$

where $\mathcal{J}_{\mathrm{m}_1} = \mathcal{J} \otimes \mathrm{m}_1$.

For $0 \leqslant s \leqslant M$, consider $X_s \in \mathcal{B}_{K_1(p)}$ such that $X_s - \sigma X_s = \omega_s$. Because of (4.4), we may assume that $X_s \equiv \sum_{u \geqslant 0} \sigma^u \omega_s \operatorname{mod}(\mathcal{B}_{K_1(p)}^{(v_0)} + \mathcal{J}_{K_1(p)}^2)$. Notice that

$$\bar{X} \equiv \sum_{r+s=M} \sigma^r (X_s) \operatorname{mod} \mathcal{J}_{K_1(p)}^2,$$

and after replacing the infinite sum $\sum_{u \geqslant 0}$ by its first $(N^* - s)$ terms in the above congruence for X_s, we obtain

$$\bar{X} = \sum_{\substack{u+s \geqslant M \\ u < N^*}} \sigma^u \omega_s \operatorname{mod}(\mathcal{B}_{K_1(p)}^{(v_0)} + \mathcal{J}_{K_1(p)}^2 + t_1^{Cp^M q} \mathcal{J}_{\mathrm{m}_1}). \tag{4.5}$$

4.6. The study of $\boldsymbol{X}$. From the above formulas (4.4) it follows that $\bar{X}$ and $\sigma(\bar{X})$ belong to $\mathcal{B}^{(v_0)}_{K_1(p)} + t_1^{Cp^M}\mathcal{J}_{\mathrm{m}_1} + \mathcal{J}^2_{K_1(p)}$. This implies that

$$\omega\sigma(\bar{X}) \in \mathcal{B}^{(v_0)}_{K_1(p)}\mathcal{J}_{K_1(p)} + \mathcal{J}_{\mathrm{m}_1}.$$

Therefore, when solving equation (4.3) for X, this term will not have any influence on the field of definition of $X \bmod \mathcal{B}^{(v_0)}_{K_1(p)}\mathcal{J}_{K_1(p)}$.

For a similar reason, we may replace $\bar{X}$ in (4.3) by the right hand side from (4.5) without affecting the field of definition of $X \bmod \mathcal{B}^{(v_0)}_{K_1(p)}\mathcal{J}_{K_1(p)}$. The new right hand side will be then equal to

$$\sum_{\substack{a\in\mathbb{Z}^0(p)\\ 0\leqslant s\leqslant M}} t_1^{-ap^Mq}\mathcal{E}_s(a,\Theta^{*p^{M-s}}) - \sum_{\substack{a_1,a_2\in\mathbb{Z}^0(p)\\ 0\leqslant s\leqslant M}} t_1^{-(a_1+a_2)p^Mq}\mathcal{E}_s(a_1,\Theta^{*p^{M-s}})D_{a_1M}D_{a_2M}$$
$$- \sum_{\substack{0\leqslant s_1\leqslant M, a_1,a_2\in\mathbb{Z}^0(p)\\ N^*>u>M-s_1}} t_1^{-a_1p^{s_1+u}q-a_2p^Mq}\mathcal{E}_{s_1}(a_1,\Theta^{*p^u})[D_{a_1,s_1+u},D_{a_2,M}].$$

Finally we can apply the Witt-Artin-Schreier equivalence to the last formula to deduce that modulo any ideal containing the ideal $\mathcal{B}^{(v_0)}_{K_1(p)}\mathcal{J}_{K_1(p)}$, the elements X and X', where $X'-\sigma X'=$

$$\sum_{0\leqslant s\leqslant M} t_1^{-ap^sq}\mathcal{E}_s(a_1,\Theta^*)D_{as} - \sum_{0\leqslant s\leqslant M} t_1^{-(a_1+a_2)p^sq}\mathcal{E}_s(a_1,\Theta^*)D_{a_1s}D_{a_2s}$$
$$- \sum_{\substack{0\leqslant s_1\leqslant M\\ M-N^*<s_2<s_1}} t_1^{-(a_1p^{s_1}+a_2p^{s_2})q}\mathcal{E}_{s_1}(a,\Theta^*)[D_{a_1s_1},D_{a_2s_2}]$$

have the same field of definition.

We can use this relation to find the minimal ideal I in $\mathcal{B}$ such that $X \bmod I_{K_1(p)}$ is defined over an extension of K_1 with upper ramification number less than $qv_0 - r^*(q-1)$. Indeed, we know that $I \bmod \mathcal{J}^2 = \mathcal{B}^{(v_0)} \bmod \mathcal{J}^2$ and therefore, we may always assume that $I \supset \mathcal{B}^{(v_0)}\mathcal{J}$. As before, we are also allowed to change the right hand side of (4.6) by any element of $\mathcal{B}\otimes\mathcal{J}_{\mathrm{m}_1}$. We may always assume that $I \supset \mathcal{B}(v)$ for any $v > v_0$, because I must contain all $\mathcal{B}^{(v)}$ with $v > v_0$ and, by the inductive assumption, $\mathcal{B}^{(v)}$ coincides with $\mathcal{B}(v)$. So, we can assume that I contains the ideal $\mathcal{B}^{(v_0+)}$ generated by $\mathcal{B}^{(v_0)}\mathcal{J}$ and all $\mathcal{B}^{(v)}$ with $v > v_0$.

4.7. Final simplification of (4.6)**.** For $0 \leqslant s \leqslant M$, consider the identity $\mathcal{E}_s(a, \Theta^*) = p^s a t_1^{r^*(q-1)} + p^s t_1^{2r^*(q-1)} g_r(t_1)$ from Subsection 4.5.

Lemma 4.6. $p^s t_1^{-(a_1+a_2)p^s q + 2r^*(q-1)} D_{a_1 s} D_{a_2 s} \in \mathcal{B}_{K_1}^{(v_0)} \mathcal{J}_{K_1} + \mathcal{J}_{\mathrm{m}_1}$.

Proof. Indeed, if $p^s a_1 \geqslant v_0$ (resp. if $p^s a_2 \geqslant v_0$) then $p^s D_{a_1 s}$ (resp. $p^s D_{a_2 s}$) belongs to $\mathcal{B}_k^{(v_0)} \bmod \mathcal{J}_k^2$.

If both $p^s a_1, p^s a_2$ are less than v_0 then we use the fact that

$$-(a_1 + a_2)p^s q + 2r^*(q-1) > Cp^M + Cp^M > 0,$$

cf. Subsubsection 4.3.4, to conclude that the corresponding term belongs to $\mathcal{J}_{\mathrm{m}_1}$.

The lemma is proved □

The following lemma deals with the terms coming from the third sum and can be proved similarly.

Lemma 4.7. $p^{s_1} t_1^{-(p^{s_1} a_1 + p^{s_2} a_2)q + 2r^*(q-1)} [D_{a_1 s_1}, D_{a_2 s_2}] \in \mathcal{B}_{K_1}^{(v_0)} \mathcal{J}_{K_1} + \mathcal{J}_{\mathrm{m}_1}$.

The next lemma deals with the terms coming from the first sum.

Lemma 4.8. $p^s t_1^{-ap^s q + 2r^*(q-1)} D_{as} \in \mathcal{B}_{K_1}^{(v_0+)} + \mathcal{J}_{\mathrm{m}_1}$.

Proof. There is nothing to prove if $-ap^s q + 2r^*(q-1) > 0$.

Assume now that $ap^s q \geqslant 2r^*(q-1)$. Consider the expression for $\mathcal{F}_{ap^s}$, cf. Subsection 4.2. Notice that $ap^s > v_0$ (use estimate c) from n.4.3.4) and, therefore, $\mathcal{F}_{ap^s} \in \mathcal{B}_k(ap^s) = \mathcal{B}_k^{(ap^s)}$.

It will be sufficient to show that any term of degree 2 in the expression of $\mathcal{F}_{ap^s}$ belongs to $\mathcal{B}_k^{(v_0)} \mathcal{J}_k$. Indeed, it then follows that the linear term $p^s a D_{as}$ of $\mathcal{F}_{ap^s}$ belongs to $\mathcal{B}_k^{(ap^s)} + \mathcal{B}_k^{(v_0)} \mathcal{J}_k \subset \mathcal{B}_k^{(v_0+)}$ and the statement of our lemma is proved.

In order to prove this property of degree 2 terms notice that all of them contain as a factor either a product $p^{s_1} D_{a_1 s_1} D_{a_2 s_2}$ or a product $p^{s_1} D_{a_2 s_2} D_{a_1 s_1}$, where $s_1 \geqslant s_2$ and $p^{s_1} a_1 + p^{s_2} a_2 = p^s a$. Then we have the following two cases:

(1) if either $p^{s_1} a_1 \geqslant v_0$ or $p^{s_1} a_2 \geqslant v_0$ then this product belongs to $\mathcal{B}_k^{(v_0)} \mathcal{J}_k$;

(2) if both $p^{s_1} a_1$ and $p^{s_1} a_2$ are less than v_0, then $p^{s_1} a_1 < v_0 - \delta_1$ and $p^{s_2} a_2 \leqslant p^{s_1} a_2 < v_0 - \delta_1$. Therefore,

$$2r^*(q-1) \leqslant p^s a q = (p^{s_1} a_1 + p^{s_2} a_2) q < 2q(v_0 - \delta_1).$$

This contradicts the assumption a) from Subsubsection 4.3.4.

The lemma is completely proved. □

By the above three lemmas, we can everywhere replace the factors $\mathcal{E}_s(a,\Theta^*)$ by $p^s a t_1^{r^*(q-1)}$ and, therefore, the right hand side of (4.6) is congruent modulo $\mathcal{B}_{K_1}^{(v_0+)}+\mathcal{J}_{\mathrm{m}_1}$ to the sum $\sum_{\gamma\geqslant 0} t_1^{-q\gamma+r^*(q-1)}\mathcal{F}'_\gamma$, where $\mathcal{F}'_\gamma$ is given by the same formula as $\mathcal{F}_\gamma$, cf. Subsection 4.2, but with the additional restriction $n_2>M-N^*$ in the last sum.

Lemma 4.9. *If $\gamma\geqslant v_0$ then $\mathcal{F}'_\gamma\equiv\mathcal{F}_\gamma \operatorname{mod}\mathcal{B}_k^{(v_0)}\mathcal{J}_k$.*

Proof. Suppose the term $p^{n_1}a_1[D_{a_1n_1},D_{a_2n_2}]$ enters into the formula for $\mathcal{F}_\gamma$ but does not enter into the formula for $\mathcal{F}'_\gamma$.

Then $a_1,a_2\leqslant C$, $p^{n_1}a_1+p^{n_2}a_2=\gamma\geqslant v_0$ and $n_2\leqslant M-N^*$. Then

$$p^{n_1}a_1=\gamma-p^{n_2}a_2\geqslant v_0-p^Mq^{-1}C>r^*(1-q^{-1})-p^Mq^{-1}C>v_0-\delta_1$$

(use 4.3.2 a)). Therefore, $p^{n_1}a_1\geqslant v_0$, $p^{n_1}D_{a_1n_1}\in\mathcal{B}_k^{(v_0)}\mathcal{J}_k^2$ and $p^{n_1}a_1[D_{a_1n_1},D_{a_2n_2}]\in\mathcal{B}_k^{(v_0)}\mathcal{J}_k$.

The lemma is proved. □

Now notice that:

- if $\gamma>v_0$, then the term $t_1^{-q\gamma+r^*(q-1)}\mathcal{F}_\gamma$ belongs to $\mathcal{B}_{K_1}(\gamma)=\mathcal{B}_{K_1}^{(\gamma)}$;
- if $\gamma<v_0$, then the term $t_1^{-q\gamma+r^*(q-1)}\mathcal{F}'_\gamma$ belongs to $\mathcal{J}_{\mathrm{m}_1}$.

So, the ideal $\mathcal{B}^{(v_0)}$ appears as the minimal ideal I of $\mathcal{B}$ such that I contains the ideal $\mathcal{B}^{(v_0+)}$ and such that the largest upper ramification number of the field of definition over K_1 of the solution $X''\in\mathcal{B}_{K_1(p)}\operatorname{mod}I_{K_1(p)}$ of the equation

$$X''-\sigma X''=\mathcal{F}_{v_0}t_1^{-qv_0+r^*(q-1)}\operatorname{mod}I_{K_1(p)}$$

is less than $qv_0-r^*(q-1)$.

It only remains to notice that $p\mathcal{F}_{v_0}\in\mathcal{B}_k^{(v_0+)}$, and if $\mathcal{F}_{v_0}\notin I_k$ then the upper ramification number of the field of definition $K_1(X'',I)$ over K_1 is equal to $qv_0-r^*(q-1)$.

The theorem is proved.

5. Compatibility with ramification filtration

In this section with the notation from Section 1, $A=\mathcal{A}\operatorname{mod}\mathcal{J}^3$, $A_k=A\otimes W(k)$. For any $v\geqslant 0$, $A^{(v)}=\mathcal{A}^{(v)}\operatorname{mod}\mathcal{J}^3$, $A_k^{(v)}:=A^{(v)}\otimes W(k)$. We also set $J=\mathcal{J}\operatorname{mod}\mathcal{J}^3$ with the corresponding extension of scalars $J_k=J\otimes W(k)$. Suppose f is a continuous automorphism of the $\mathbb{Z}_p$-algebra A such that, for any $v\geqslant 0$, $f(A^{(v)})=A^{(v)}$. Consider the identification $\mathcal{J}\operatorname{mod}\mathcal{J}^2=\Gamma(p)^{\mathrm{ab}}$ from part b) of proposition 1.2 and denote again by f the continuous automorphism of $\mathcal{M}=I(p)^{\mathrm{ab}}\operatorname{mod}p$ induced by f. Consider the standard topological generators D_{an}, $a \in \mathbb{Z}(p), n \in \mathbb{Z} \bmod N_0$, for $\mathcal{M}$ and set, for any $a \in \mathbb{Z}(p)$,

$$f(D_{a0}) = \sum_{b,m} \alpha_{abm}(f) D_{bm},$$

where the coefficients $\alpha_{abm}(f) \in k$. With the above notation, the principal results of this section are:

if $\alpha_{110}(f) \neq 0$ and $N_0 \geqslant 3$ then

- there is an $\eta \in \mathrm{Aut}^0 K$ such that for any $a, b \in \mathbb{Z}(p)$ and $a \leqslant b < p^{N_0-3}$, it holds $\alpha_{ab0}(f) = \alpha_{ab0}(\eta^*)$;

- if $a \leqslant b < p^{N_0-3}$ and $m \in \mathbb{N}$ is such that $b/p^m < a$ then $\alpha_{a,b,-m \bmod N_0}(f) = 0$.

5.1. The elements $\mathcal{F}_\gamma(v)$. By Theorem B, cf. Subsection 4.2, for any $v \geqslant 0$, the ideal $A_k^{(v)}$ is the minimal closed σ-invariant ideal in A_k containing the explicitly given elements $\mathcal{F}_\gamma$, for all $\gamma \geqslant v$. For any $a \in \mathbb{Z}(p)$ and $n \in \mathbb{Z} \bmod N_0$, set $\Delta_{a0} = (1/a)\mathcal{F}_a$ and $\Delta_{an} = \sigma^n \Delta_{a0}$. Then $\Delta_{an} \equiv D_{an} \bmod \mathcal{J}_k^2$ and $\{\Delta_{an} \mid a \in \mathbb{Z}(p), n \in \mathbb{Z} \bmod N_0\} \cup \{D_0\}$ is a new system of topological generators for A_k. The elements of this new set of generators together with their pairwise products form a topological basis of the $W(k)$-module A_k.

For any $\gamma \geqslant v \geqslant 0$, consider the following elements $\mathcal{F}_\gamma(v)$ (these elements have already been mentioned in Subsection 4.2):

If $\gamma = ap^m$ with $a \in \mathbb{Z}(p)$ and $m \in \mathbb{Z}_{\geqslant 0}$ set

$$\mathcal{F}_\gamma(v) = p^m a \Delta_{am} - \sum_{\substack{n \geqslant 0, a_1, a_2 \in \mathbb{Z}(p) \\ p^n(a_1+a_2)=\gamma \\ p^n a_1, p^n a_2 < v}} p^n a_1 \Delta_{a_1 n} \Delta_{a_2 n};$$

If $\gamma \notin \mathbb{Z}$ set

$$\mathcal{F}_\gamma(v) = - \sum_{\substack{n_1 \geqslant 0, a_1, a_2 \in \mathbb{Z}(p) \\ p^{n_1} a_1 + p^{n_2} a_2 = \gamma \\ p^{n_1} a_1, p^{n_1} a_2 < v}} p^{n_1} a_1 [\Delta_{a_1 n_1}, \Delta_{a_2 n_2}].$$

Similarly to Subsection 4.2, we have the following property.

Proposition 5.1. *For any $v \geqslant 0$, $A_k^{(v)}$ is the minimal σ-invariant closed ideal of A_k containing the elements $\mathcal{F}_\gamma(v)$ for all $\gamma \geqslant v$.*

5.2. The submodules $A^{(v)}_{\mathrm{tr}}$ and $A^{(v)}_{\mathrm{adm}}$. Suppose $v\geqslant 0$.

Let $A^{(v)}_{\mathrm{tr}}$ be the $W(k)$-submodule in A_k generated by the following elements:

tr$_1$) $p^s\Delta_{an}$ with $s\geqslant 0$ and $p^sa\geqslant 2v$;

tr$_2$) $p^s\Delta_{a_1n_1}\Delta_{a_2n_2}$ with $a_1,a_2\in\mathbb{Z}(p)$, $s\geqslant 0$ and $n_1,n_2\in\mathbb{Z}\operatorname{mod}N_0$ such that $\max\{p^sa_1,p^sa_2\}\geqslant v$.

Let $A^{(v)}_{\mathrm{adm}}$ be the minimal closed $W(k)$-submodule in A_k containing $A^{(v)}_{\mathrm{tr}}$ and the following elements:

adm$_1$) $p^s\Delta_{an}$, with $s\geqslant 0$, $a\in\mathbb{Z}(p)$ and $p^sa\geqslant v$;

adm$_2$) $p^s\Delta_{a_1n_1}\Delta_{a_2n_2}$, where $a_1,a_2\in\mathbb{Z}(p)$, $n_1,n_2\in\mathbb{Z}\operatorname{mod}N_0$ and $s=s(a_1,a_2)\in\mathbb{Z}_{\geqslant 0}$ are such that:

(1) $v/p\leqslant\max\{p^sa_1,p^sa_2\}<v$;

(2) $\max\left\{p^s\left(a_1+\frac{a_2}{p^{n_{12}}}\right),p^s\left(\frac{a_1}{p^{n_{21}}}+a_2\right)\right\}\geqslant v$, where $0\leqslant n_{12},n_{21}<N_0$, $n_{12}\equiv n_1-n_2\operatorname{mod}N_0$ and $n_{21}\equiv n_2-n_1\operatorname{mod}N_0$;

(3) if $n_1=n_2$ then $a_1+a_2\equiv 0\operatorname{mod}p$.

Proposition 5.2. *For any $v\geqslant 0$,*
1) $f(A^{(v)}_{\mathrm{tr}})=A^{(v)}_{\mathrm{tr}}$*;*
2) $A^{(v)}_{\mathrm{adm}}\supset A^{(v)}_k\supset A^{(v)}_{\mathrm{tr}}\supset pA^{(v)}_{\mathrm{adm}}$*;*
3) *the elements from* adm$_1$) *and* adm$_2$) *form a k-basis of* $A^{(v)}_{\mathrm{adm}}\operatorname{mod}A^{(v)}_{\mathrm{tr}}$*.*

Proof. 1) It is sufficient to notice that $A^{(v)}_{\mathrm{tr}}$ is the minimal σ-invariant $W(k)$-submodule in A containing $\sum_{\gamma\geqslant 2v}\mathcal{F}_\gamma(v)W(k)+\sum_{\gamma\geqslant v}\mathcal{F}_\gamma(v)J_k$.

2) From the above n.1) it follows that $A^{(v)}_k\supset A^{(v)}_{\mathrm{tr}}$. The embedding $A^{(v)}_k\subset A^{(v)}_{\mathrm{adm}}$ follows from the definition of $A^{(v)}_{\mathrm{adm}}$: as a matter of fact, $A^{(v)}_{\mathrm{tr}}$ is spanned by all summands of elements $\sigma^s\mathcal{F}_\gamma$ with $s\in\mathbb{Z}\operatorname{mod}N_0$ and $\gamma\geqslant v$. The embedding $pA^{(v)}_{\mathrm{adm}}\subset A^{(v)}_{\mathrm{tr}}$ follows from the fact that each element listed in adm$_1$) and adm$_2$) belongs to $A^{(v)}_{\mathrm{tr}}$ after multiplication by p.

3) It is easy to see that any k-linear combination of the elements from adm$_1$) and adm$_2$) does not belong to $A^{(v)}_{\mathrm{tr}}\operatorname{mod}pA^{(v)}_{\mathrm{adm}}$. ∎

Proposition 5.3. *Suppose $v\geqslant 0$ and $p^s\Delta_{a_1n_1}\Delta_{a_2n_2}$ is one of elements listed in* adm$_2$)*. Let $n=\min\{n_{12},n_{21}\}$. If*

$$v/p^{N_0-n}\leqslant d(v):=\min\{v-a\mid a\in\mathbb{Z},a<v\}$$

then there are unique $m\in\mathbb{Z}\operatorname{mod}N_0$ and $\gamma\geqslant v$ such that $p^sa_1\Delta_{a_1n_1}\Delta_{a_2n_2}$ appears (with non-zero coefficient) in the expression of $\sigma^m\mathcal{F}_\gamma(v)$.

Remark. We are going to apply this proposition in the following situations:

(1) $v \in \mathbb{N}$, $v < p^{N_0}$, $n_1 = n_2 = 0$;

(2) $v = c + 1/p$, $n_1 = 0$, $n_2 = -1$, where $c \in \mathbb{N}$ and $c < p^{N_0-2}$.

Proof. By symmetry we may assume that $n = n_{12}$.

If $n_{12} \neq 0$ we have $p^s\left(a_1 + \frac{a_2}{p^n}\right) = \gamma \geqslant v$, because of property adm$_2$)(2), and

$$p^s\left(\frac{a_1}{p^{N_0-n}} + a_2\right) < \frac{v}{p^{N_0-n}} + p^s a_2 \leqslant d(v) + (v - d(v)) = v \leqslant \gamma.$$

Therefore, the term $p^s\Delta_{a_1n_1}\Delta_{a_2n_2}$ appears in the expression of $\sigma^{n_1-s}\mathcal{F}_\gamma(v)$. This term will appear in the expression of another $\sigma^{n'}\mathcal{F}_{\gamma'}(v)$, where $\gamma' \geqslant v$, if and only if $p^s\left(a_1 + \frac{a_2}{p^{n+mN_0}}\right) \geqslant v$ or $p^s\left(\frac{a_1}{p^{mN_0-n}} + a_2\right) \geqslant v$, where $m \in \mathbb{N}$. But the condition $v/p^{N_0-n} < d(v)$ implies that all such numbers are less than v.

If $n_{12} = 0$ then $\gamma = p^s(a_1 + a_2) \geqslant v$ and $p^s\Delta_{a_1n_1}\Delta_{a_2n_2}$ appears in the expression of $\sigma^{n_1-s}\mathcal{F}_\gamma(v)$. This element can appear in the expression of another $\sigma^{n'}\mathcal{F}_{\gamma'}(v)$, where $\gamma' \geqslant v$, if and only if $\gamma' = p^s\left(a_1 + \frac{a_2}{p^{mN_0}}\right) \geqslant v$ or $\gamma' = p^s\left(\frac{a_1}{p^{mN_0}} + a_2\right) \geqslant v$, where $m \in \mathbb{N}$. As earlier, $\gamma' < v$ in both cases.

The proposition is proved. $\square$

Remark. If $v/p^{N_0/2} < d(v)$, then elements of the set

$$\{\sigma^s\mathcal{F}_\gamma^{(v)} \bmod A_{\mathrm{adm}}^{(v)} \mid 0 \leqslant s < N_0, \gamma \geqslant v\}$$

are linear combinations of disjoint groups of elements listed in adm$_1$) and adm$_2$).

5.3. Denote by the same symbol f the morphism of $W(k)$-modules

$$A^{(v)} \bmod A_{\mathrm{tr}}^{(v)} \longrightarrow A^{(v)} \bmod A_{\mathrm{tr}}^{(v)},$$

which is induced by $f : A \longrightarrow A$. As earlier, denote again by f the k-linear extension of the automorphism of $\mathcal{M}$, which is induced by f. Because the images of D_{an} and Δ_{an} coincide in $\mathcal{M}_k$, we have, for any $a \in \mathbb{Z}(p)$,

$$f(\Delta_{a0}) = \sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z} \bmod N_0}} \alpha_{abm}(f)\Delta_{bm}.$$

It will be convenient sometimes to set $\alpha_{ab0}(f) = 0$ if a or b are divisible by p.

Proposition 5.4. *Suppose $\alpha_{110}(f) = \alpha \in k^*$. Then $\alpha_{aa0}(f) = \alpha^a$, for any $a \in \mathbb{Z}(p)$ such that $a < p^{N_0-1}$ if $p \neq 2$ and $N_0 \geqslant 2$, and such that $a < 2^{N_0}$ if $p = 2$ and $N_0 \geqslant 3$.*

Proof. By proposition 5.3, for any $v \leqslant p^{N_0}$ such that $v \equiv 0 \bmod p$, the formula for $f(\mathcal{F}_v(v)) \bmod A_{\mathrm{tr}}^{(v)}$ must contain all terms $a_1\Delta_{a_10}\Delta_{a_20}$, for which $a_1 + a_2 = v$, and the term $p^s a\Delta_{as}$, where $p^s a = v$ and $a \in \mathbb{Z}(p)$, with the same coefficient. In other words, for such indices $a_1, a_2, a \in \mathbb{Z}(p)$,

$$\alpha_{a_1a_10}(f)\alpha_{a_2a_20}(f) = \sigma^s\alpha_{aa0}(f). \tag{5.1}$$

For $a \in \mathbb{Z}(p)$, $a < p^{N_0}$, set $\gamma(a) = \alpha_{aa0}(f)\alpha_{110}(f)^{-1}$. Then $\gamma(1) = 1$ and $\gamma(a_1)\gamma(a_2) = \gamma(a)^{p^s}$ if $a_1 + a_2 = p^s a$.

Suppose $p \neq 2$.

First, we prove that for $n \in \mathbb{Z}(p)$ satisfying $1 \leqslant n < p^{N_0-1}$, we have

$$\gamma(n) = \gamma(2)^{n-1}. \tag{5.2}$$

This is obviously true for $n = 1$ and $n = 2$.

Assume that $n \geqslant 2$ and that $\gamma(m) = \gamma(2)^{m-1}$ holds for all $m \in \mathbb{Z}(p)$ such that $m \leqslant n$. Consider a special case of relation (5.1) with $n \in \mathbb{Z}(p)$

$$\gamma(1)\gamma(np - 1) = \gamma(n)^p. \tag{5.3}$$

If $n \not\equiv -1 \bmod p$ then use the relation $\gamma(p-1)\gamma(p+1) = \gamma(2)^p$, which is again a special case of (5.1), to deduce from (5.3) that

$$\gamma(n+1) = \gamma(1)\gamma(n+1) = \gamma(n)\gamma(2) = \gamma(2)^n.$$

If $n \equiv -1 \bmod p$ and $p \neq 3$ then $n \geqslant 4$ and by the inductive assumption $\gamma(3) = \gamma(2)^2$. Apply the relation $\gamma(p-1)\gamma(2p+1) = \gamma(3)^p = \gamma(2)^{2p}$ to deduce from (5.3) that

$$\gamma(n+1) = \gamma(1)\gamma(n+2) = \gamma(n)\gamma(2)^2 = \gamma(2)^{n+1}.$$

If $p = 3$ then $\gamma(p-1)\gamma(2p+1) = \gamma(1)^{p^2}$ and we obtain from (5.3) that

$$\gamma(n+1) = \gamma(1)\gamma(n+2) = \gamma(n) = \gamma(2)^{n-1} = \gamma(2)^{n+1},$$

because $\gamma(2) = 1$ (using that $\gamma(1)\gamma(2) = \gamma(1)^3$).

So, relation (5.2) is proved.

Still assuming that $p \neq 2$ prove that $\gamma(2) = 1$. The relation $\gamma(1)\gamma(p-1) = \gamma(1)^p$ implies that $\gamma(2)^{p-2} = \gamma(p-1) = 1$. The equality $\gamma(1)\gamma(p^2-1) = \gamma(1)^{p^2}$ implies that $\gamma(2)^{p^2-2} = \gamma(p^2-1) = 1$. Then $\gamma(2) = 1$ because $p^2 - 2$ and $p - 2$ are coprime. This completes the case $p \neq 2$.

Consider now the case $p = 2$.

Notice that for any $n \in \mathbb{Z}(2)$ such that $1 < n < 2^{N_0}$, we have $n+1 = 2^s a$, where $a \in \mathbb{Z}(2)$, $s \in \mathbb{N}$ and $a < n$. Therefore, $\gamma(1)\gamma(n) = \gamma(a)^{2^s}$ and the equality $\gamma(n) = 1$ follows by induction on $n \geqslant 1$ for all $n < 2^{N_0}$. ☐

Corollary 5.5. *If $\alpha_{110}(f) = 1$ then $\alpha_{aa0}(f) = 1$ whenever $a < p^{N_0-1}$, $p \neq 2$ or $a < 2^{N_0}$, $p = 2$.*

Proposition 5.6. *Suppose $N_0 \geqslant 3$, $\alpha_{110}(f) \in k^*$, $a, b \in \mathbb{Z}(p)$, $a, b < p^{N_0-2}$. If $0 \leqslant m < N_0$ and $b/p^m < a$ then $\alpha_{a,b,-m \bmod N_0}(f) = 0$.*

Proof. For a given $b\in\mathbb{Z}(p)$, $b<p^{N_0-2}$ and $1\leqslant m<N_0$, let $a\in\mathbb{Z}(p)$ be the minimal integer such that $\alpha_{a',b,-m}(f)=0$ if $a'>a$. If such an a does not exist then $\alpha_{a,b,-m}(f)=0$ for all a and there is nothing to prove.

If $p\neq 2$ put $v=p^{N_0-1}$ and consider $f(\mathcal{F}_v(v))\bmod(A_{\mathrm{tr}}^{(v)}+pA_{\mathrm{adm}}^{(v)})$.

We prove that the term $\Delta_{v-a,0}\Delta_{b,-m}$ enters in $f(\mathcal{F}_v(v))$ with the coefficient

$$(v-a)\alpha_{v-a,v-a,0}(f)\alpha_{a,b,-m}(f)=-a\alpha_{v-a,v-a,0}(f)\alpha_{a,b,-m}(f). \tag{5.4}$$

Indeed, $\mathcal{F}_v(v)\bmod(A_{\mathrm{tr}}^{(v)}+pA_{\mathrm{adm}}^{(v)})$ is a sum of the terms of the form $a_1\Delta_{a_10}\Delta_{a_20}$ with $a_1,a_2\in\mathbb{Z}(p)$ such that $a_1+a_2=v$. Therefore, $f(a_1\Delta_{a_10}\Delta_{a_20})$ contains $\Delta_{v-a,0}\Delta_{b,-m}$ with coefficient

$$a_1\alpha_{a_1,v-a,0}(f)\alpha_{a_2,b,-m}(f).$$

Now notice that $\alpha_{a_2,b,-m}(f)=0$ if $a_2>a$, and $\alpha_{a_1,v-a,0}(f)=0$ if $a_1>v-a$ or, equivalently, if $a_2<a$. So, $a_1=v-a$ and the coefficient is given by formula (5.4).

By the choice of a, the coefficient (5.4) is not zero. Therefore, $\Delta_{v-a,0}\Delta_{b,-m}\in A_{\mathrm{adm}}^{(v)}$. Notice that

$$\max\left\{v-a+\frac{b}{p^m},\frac{v-a}{p^{N_0-m}}+b\right\}=v-a+\frac{b}{p^m}$$

and $b/p^m\geqslant a$. Indeed, we can use that

$$\frac{v-a}{p^{N_0-m}}+b<\frac{p^{N_0-1}}{p}+p^{N_0-2}<2p^{N_0-2}<p^{N_0-1}-p^{N_0-2}<v-a+\frac{b}{p^m}.$$

Therefore, $v-a+b/p^m\geqslant v$, i.e. $b/p^m\geqslant a$ and the proposition is proved in the case $p\neq 2$.

If $p=2$ we can take $v=2^{N_0}$ and repeat the above arguments by using in the last step the inequality

$$\frac{v-a}{2^{N_0-m}}+b<\frac{2^{N_0}}{2}+2^{N_0-2}<2^{N_0}-a\left(1-\frac{1}{2^m}\right)\leqslant v-a+\frac{b}{2^m}.$$

The proposition is completely proved. □

5.4. Suppose $r\in\mathbb{N}$ is such that $\alpha_{aa'0}(f)=0$ for any $a,a'\in\mathbb{Z}(p)$ such that $a<a'<a+r<p^{N_0-2}$.

Let $\delta(p)$ be p if $p\neq 2$ and $\delta(p)=4$ if $p=2$.

Proposition 5.7. *Assume that $\alpha_{110}(f)=1$. If $b,b_1\in\mathbb{Z}(p)$, $b_1=b+r$ and $b_1+\delta(p)<p^{N_0-2}$ then $\alpha_{bb_10}(f)=\alpha_{b-\delta(p),b_1-\delta(p),0}(f)$.*

Proof. Let $a_0=p^{N_0-2}-1$, $v_0=a_0+1/p$, $v=a_0+\frac{b}{p}$. We need the following lemma.

Lemma 5.8. *If $a',b',c\leqslant a_0$ and $a'+b'/p=v$ then $\alpha_{a',c,-1}(f)=0$.*

Proof. It follows from the inequalities

$$\frac{c}{p} \leqslant \frac{a_0}{p} \leqslant a_0 - \frac{a_0}{p} < v - \frac{b'}{p} = a'$$

and proposition 5.6. □

We continue the proof of proposition 5.7. Consider

$$\mathcal{F}_v(v_0) = -\sum_{\substack{a'+b'/p=v\\ a',b'\leqslant a_0}} a'[\Delta_{a'0}, \Delta_{b',-1}] \operatorname{mod} pA^{(v)}_{\mathrm{adm}}.$$

Using that $v_0/p^{N_0-1} < d(v_0) = 1/p$, cf. proposition 5.3, we can find now the coefficient for $[\Delta_{a_0 0}, \Delta_{b_1,-1}]$ in $f(\mathcal{F}_v(v_0))$. By the above lemma $\alpha_{a',b,-1}(f) = 0$, therefore the image of the term $a'[\Delta_{a'0}, \Delta_{b',-1}]$ gives a coefficient

$$a'\alpha_{a'a_0 0}(f)\sigma^{-1}(\alpha_{b'b_1 0}(f)).$$

If $a' < a_0$ and $\alpha_{a'a_0 0}(f) \neq 0$ then $a' \leqslant a_0 - r$, $b' \geqslant b + rp > b_1$ and $\alpha_{b'b_1 0}(f) = 0$. So, the coefficient is non-zero only for $a' = a_0$. Then by Corollary 5.5 $\alpha_{a'a_0 0}(f) = 1$ and the coefficient will be equal to $a_0\sigma^{-1}(\alpha_{bb_1 0}(f))$.

If $p \neq 2$ we can proceed similarly to find the coefficient for $[\Delta_{a_0-1,0}, \Delta_{b_1+p,-1}]$ in $f(\mathcal{F}_v(v_0))$. It equals $(a_0 - 1)\sigma^{-1}(\alpha_{b+p,b_1+p,0}(f))$. Therefore, by proposition 5.3

$$\alpha_{bb_1 0}(f) = \alpha_{b+p,b_1+p,0}(f)$$

and the case $p \neq 2$ is completely considered.

If $p = 2$, we similarly find similarly the coefficient for $[\Delta_{a_0-2,0}, \Delta_{b_1+4,-1}]$ in $f(\mathcal{F}_v(v_0))$. It equals $(a_0 - 2)\sigma^{-1}(\alpha_{b+4,b_1+4,0}(f))$ and we obtain

$$\alpha_{bb_1 0}(f) = \alpha_{b+4,b_1+4,0}(f).$$

The proposition is proved. □

5.5. Now we come to the central point of this section.

Proposition 5.9. *Suppose $\alpha_{110}(f) \neq 0$ and $N_0 \geqslant 3$. Then there is an $\eta \in \mathrm{Aut}^0 K$ such that $\alpha_{ab0}(f\eta^*) = \delta_{ab}$, for any $a, b \in \mathbb{Z}(p)$ with $a \leqslant b < p^{N_0-3}$, where δ_{ab} is the Kronecker symbol.*

Proof. Proposition 5.4 together with part 2) of proposition 2.1 imply that after replacing f by $f\eta^*$ for some $\eta \in \mathrm{Aut}^0 K$ such that $\eta(t) = \alpha_{110}(f)t$, we can assume that $\alpha_{aa0}(f) = 1$ if $a < p^{N_0-1}$.

Let $r = r(f) \in \mathbb{N}$ be the maximal subject to the condition that $\alpha_{ab0}(f) = 0$, for any $a, b \in \mathbb{Z}(p)$ with $a, b < p^{N_0-2}$ and $a < b < a + r$.

If $r \geqslant p^{N_0-3} - 1$ then there is nothing to prove. Therefore, we can assume that $r \leqslant p^{N_0-3} - 2$. For $1 \leqslant a < p^{N_0-2}$, set $\alpha_a(r) = \alpha_{a,a+r,0}(f)$ if $a \in \mathbb{Z}(p)$ and $\alpha_a(r) = 0$, otherwise.

By proposition 5.7 $\alpha_a(r)$ depends only on the residue $a \bmod \delta(p)$ and by the choice of r the function $a \mapsto \alpha_a(r)$ is not identically zero. The proposition will be proved if we show the existence of $\eta \in \mathrm{Aut}^0 K$ such that $r(f\eta^*) > r(f)$.

In the case $p \neq 2$ apply proposition 2.5 with $w_0 = 1+r$. Let η will be the corresponding character. If $r(f\eta^*) > r(f)$, then the proposition is proved. So, assume that $r(f\eta^*) = r(f)$. Therefore, by replacing f by $f\eta^*$ we can assume the following normalisation conditions:

a) $\alpha_1(r) = 0$ if $r \not\equiv -1 \bmod p$;

b) $\alpha_2(r) = 0$ if $r \equiv -1 \bmod p$.

In the case $p = 2$, apply proposition 2.6 with either $w_0 = r+2$ if $r \equiv 2 \bmod 4$ or $w_0 = r$ if $r \equiv 0 \bmod 4$. In the first case we have the normalisation condition

c) $\alpha_1(r) = \alpha_3(r) = 0$;

in the second case we obtain only that

d) $\alpha_1(r) = 0$.

The case $p \neq 2$.

If $r = p^{N_0-3} - 2$ then $\alpha_1(r) = \alpha_{ab0}(f) = 0$ if $a = 1, b = p^{N_0-3} - 1$. For all other couples $a, b \in \mathbb{Z}(p)$ such that $a < b < p^{N_0-3}$, we have $\alpha_{ab0}(f) = 0$ because $b - a < r$. Therefore, we can assume that $r \leqslant p^{N_0-3} - 3$.

Let $c_j = p(r+1)+j$ for $j = 1, 2, \dots, p-1$. Then $c_j \leqslant p(p^{N_0-3}-2)+p-1 < p^{N_0-2}$, for all j. Set $v_j = c_j + 1/p$ and consider the coefficient for $\mathcal{F}_{v_j+r}(v_j)$ in the image $f(\mathcal{F}_{v_j}(v_j)) \in A_{\mathrm{adm}}^{(v_j)} \bmod A_{\mathrm{tr}}^{(v_j)} + pA_{\mathrm{adm}}^{(v_j)}$.

Similarly to the proof of proposition 5.7, we see that the term $[\Delta_{c_j0}, \Delta_{1+rp,-1}]$ from the expression of $\mathcal{F}_{v_j+r}(v_j)$ can appear with non-zero coefficient only as image of one of the following two terms from $\mathcal{F}_{v_j}(v_j)$: $(c_j - r)[\Delta_{c_j-r,0}, \Delta_{1+rp,-1}]$ and $c_j[\Delta_{c_j0}, \Delta_{1,-1}]$. This coefficient is equal to

$$(c_j - r)\alpha_{c_j-r}(r) + c_j\alpha_{1,1+rp,0}(f).$$

Similarly, the term $[\Delta_{c_j-1,0}, \Delta_{1+(r+1)p,-1}]$ from the expression of $\mathcal{F}_{v_j+r}(v_j)$ can appear with non-zero coefficient only in the image of either $(c_j-1-r)[\Delta_{c_j-1-r,0}, \Delta_{1+(r+1)p,-1}]$ or $(c_j-1)[\Delta_{c_j-1,0}, \Delta_{1+p,-1}]$. Therefore, this coefficient will be equal to

$$(c_j - 1 - r)\alpha_{c_j-1-r}(r) + (c_j - 1)\sigma^{-1}\alpha_{1+p,1+(r+1)p,0}(f)$$

and we obtain the following relation

$$\frac{c_j - r}{c_j}\alpha_{c_j-r}(r) = \frac{c_j - 1 - r}{c_j - 1}\alpha_{c_j-1-r}(r) + X, \tag{5.5}$$

where $X = \sigma^{-1}(\alpha_{1+p,1+(r+1)p,0}(f)) - \sigma^{-1}(\alpha_{1,1+rp,0}(f))$.

For $j=1,\dots,p-1$, set $\beta_j=\frac{c_j-r}{c_j}\alpha_{j-r}(r)$. Then the above relation (5.5) implies that $\beta_2=\beta_1+X,\beta_3=\beta_2+X,\dots,\beta_{p-1}=\beta_{p-2}+X$.

The case $r\not\equiv 0 \bmod p$, $p\neq 2$.

In this case the normalisation conditions imply that

— if $r\not\equiv -1 \bmod p$ then $\beta_{r+1}=0$;

— if $r\equiv -1 \bmod p$ then $\beta_{r+2}=0$.

In both cases $\beta_r=0$. This implies that $\beta_1=\dots=\beta_{p-1}=0$. Therefore, $\alpha_a(r)=0$, for all a. This is a contradiction.

So, in the case $r\not\equiv 0 \bmod p$, $p\neq 2$ the proposition is proved.

The case $r\equiv 0 \bmod p$, $p\neq 2$

In this case we only have the normalisation condition $\beta_1=0$. Therefore, for $i=1,\dots,p-1$, we have $\beta_i=(i-1)X$ and $\alpha_a(r)=(a-1)X$ for any $a\in\mathbb{Z}(p)$, $a<p^{N_0-3}$.

Let $v=(p-1)r+p$ and consider the coefficient for $\mathcal{F}_{v+r}(v)$ in the image $f(\mathcal{F}_v(v))$. Following the images of terms of degree 2 we see that this coefficient equals $-2X$. Now notice that the linear terms in $\mathcal{F}_v(v)$ (resp. $\mathcal{F}_{v+r}(v)$) have coefficients with p-adic valuation $v_p((p-1)r+p)$ (resp. $v_p(pr+p)$). Clearly, if $1=v_p(pr+p)$ and if $1<v_p((p-1)r+p)$ then the linear term of $\mathcal{F}_{v+r}(v)$ cannot appear in the image $f(\mathcal{F}_v(v))$. Therefore, $1=v_p(pr+p)=v_p((p-1)r+p)$ and the linear terms in $\mathcal{F}_v(v)$ (resp. $\mathcal{F}_{v+r}(v)$) are multiples of $\Delta_{r+1-r/p,1}$ (resp. $\Delta_{r+1,1}$). But then $(r+1)-(r+1-r/p)=r/p<r$ and by the definition of r, $\Delta_{r+1,1}$ will not appear in the image $F(\Delta_{r+1-r/p,1})$. This contradiction proves the proposition in the case $r\equiv 0 \bmod p$, $p\neq 2$.

The case $p=2$.

Here $r\equiv 0 \bmod 2$. If $r\equiv 2 \bmod 4$ then the normalisation conditions imply that $\alpha_a(r)=0$ for all a and the proposition is proved.

If $r\equiv 0 \bmod 4$ then we only have one normalisation condition $\alpha_a(r)=0$ if $a\equiv 1 \bmod 4$. Let $\alpha_a(r)=\alpha$ where $a\equiv 3 \bmod 4$. Consider

$$\mathcal{F}_{r+4}(r+4)=(r+4)\Delta_{\frac{r+4}{2^s},s}+\sum_{a+b=r+4a,b<r+4}\Delta_{a0}\Delta_{b0}\in A_{\mathrm{adm}}^{(r+4)} \bmod A_{\mathrm{tr}}^{(r+4)},$$

where $s=v_2(r+4)\geqslant 2$. Then $f(\mathcal{F}_{r+4}(r+4))$ contains $\Delta_{r+1,0}\Delta_{r+3,0}$ with coefficient

$$\alpha_{1,r+1,0}(f)+\alpha_{3,3+r,0}(f)=\alpha,$$

and therefore it contains $\mathcal{F}_{2r+4}(r+4)$ with coefficient α. Similarly to the case $p\neq 2$, we obtain the equality $v_2(r+4)=v_2(2r+4)=2$ and consequently the fact that $f(\Delta_{r/2+1,2})$ cannot contain $\Delta_{r/4+1,2}$ with non-zero coefficient because $(r/2+1)-(r/4+1)=r/4<r$. The proposition is completely proved. $\square$

6. Proof of the main theorem — the characteristic p case

Suppose E is a field of characteristic p.

Then E' is also a field of characteristic p, because the topological groups $\Gamma_E(p)^{\mathrm{ab}}$ and $\Gamma_{E'}(p)^{\mathrm{ab}}$ are isomorphic. Looking at the ramification filtrations of these groups we deduce that the residue fields of E and E' are isomorphic. Therefore, E and E' are isomorphic complete discrete valuation fields and we can identify the maximal p-extensions $E(p)$ of E and $E'(p)$ of E'.

Let K be a finite Galois extension of E in $E(p)$. Then $E(p)$ is a maximal p-extension of K and $\Gamma_K(p)=\mathrm{Gal}(E(p)/K)$. Let K' be the extension of E' in $E(p)$ such that $g(\Gamma_K(p))=\Gamma_{K'}(p)$ (recall that g is a group isomorphism). If $s\geqslant 0$ and K_s is the unramified extension of K in $E(p)$ such that $[K_s:K]=p^s$ then $g(\Gamma_{K_s}(p))=\Gamma_{K'_s}(p)$, where K'_s is the unramified extension of K' in $E(p)$ of degree p^s. Therefore, with the notation from Section 3 we have a compatible system $g_{KK'}=\{g_{KK's}\}_{s\geqslant 0}$ of $\mathbb{F}_p$-linear continuous automorphisms $g_{KK's}:\bar{\mathcal{M}}_{Ks}\longrightarrow\bar{\mathcal{M}}_{K's}$.

Now choose uniformising elements t_K and $t_{K'}$ in K and, resp., K'. Consider the corresponding standard generators $D_{an}^{(s)}$ (resp. $D_{an}^{\prime(s)}$), where $a\in\mathbb{Z}(p)$ and $n\in\mathbb{Z}\operatorname{mod}N_s$, of $\bar{\mathcal{M}}_{Ks}=\mathcal{M}_{Ks}\hat{\otimes}_k k(p)$ (resp., $\bar{\mathcal{M}}_{K's}=\mathcal{M}_{Ks}\hat{\otimes}_k k(p)$). Here, as usual, $k\simeq\mathbb{F}_{q_0}$ is the residue field of K, $q_0=p^{N_0}$, $N_s=N_0p^s$. Then

$$g_{KK's}(D_{a0}^{(s)})=\sum_{\substack{b\in\mathbb{Z}(p)\\ m\in\mathbb{Z}\operatorname{mod}N_s}}\alpha_{abm}(g_{KK's})D_{bm}^{\prime(s)}$$

with $\alpha_{abm}(g_{KK's})\in k_s\subset k(p)$.

For each $s\geqslant 0$, choose $n_s\in\mathbb{Z}\operatorname{mod}N_s$ such that $\alpha_{11n_s}(g_{KK's})\neq 0$: n_s exists, because $g_{KK's}$ induces a $k(p)$-linear isomorphism of $\bar{\mathcal{M}}_{Ks}\operatorname{mod}\bar{\mathcal{M}}_{Ks}^{(2)}$ and $\bar{\mathcal{M}}_{K's}\operatorname{mod}\bar{\mathcal{M}}_{K's}^{(2)}$.

Let $\mathrm{Fr}(t_{K'})\in\mathrm{Aut}K'_{\mathrm{ur}}$ be such that $\mathrm{Fr}(t_{K'}):t_{K'}\mapsto t_{K'}$ and $\mathrm{Fr}(t_{K'})|_{k(p)}=\sigma$. Let $\xi\in\mathrm{Iso}^0(K'_{\mathrm{ur}},K_{\mathrm{ur}})$ be such that $\xi(t_{K'})=t_K$.

For any $s\geqslant 0$, $\mathrm{Fr}(t_{K'})$ (resp. ξ) induces a continuous field isomorphism $K'_s\longrightarrow K'_s$ (resp. $K'_s\longrightarrow K_s$). It will be denoted by $\mathrm{Fr}(t_{K'})_s$ (resp. ξ_s). With notation from n.3, we introduce continuous group isomorphisms

$$g^0_{KK's}=g_{KK's}\mathrm{Fr}(t_{K'})_s^{n_s*}:\bar{\mathcal{M}}_{Ks}\longrightarrow\bar{\mathcal{M}}_{K's}.$$

Clearly, $h_s:=g^0_{KK's}\xi_s^*$ is induced by an automorphism of $\Gamma_{K_s}(p)$ which is compatible with the ramification filtration. Notice also that, by proposition 2.1, if $a\in\mathbb{Z}(p)$, $n\in\mathbb{Z}\operatorname{mod}N_s$ and

$$h_s(D_{a0}^{(s)})=\sum_{b,m}\alpha_{abm}(h_s)D_{bm}^{(s)},$$

then $\alpha_{a,b,m-n_s}(h_s)=\sigma^{n_s}\alpha_{abm}(g_{KK's})$. In particular, $\alpha_{110}(h_s)\neq 0$. Therefore, applying proposition 5.6, we obtain that for all $s\geqslant 0$,

$$h_s\in \mathrm{Aut}_{\mathrm{adm}}\mathcal{M}_{Ks} \,\mathrm{mod}\, \mathcal{M}_{K_s}^{(p^{N_s-2})},$$

the residues $n_s\in\mathbb{Z}\,\mathrm{mod}\,N_s$ are unique, and $n_{s+1}\,\mathrm{mod}\,N_s=n_s$. Here we use that $D_{an}^{(s+1)}\mapsto D_{an}^{(s)}$ under the natural morphism from $\bar{\mathcal{M}}_{K,s+1}$ to $\bar{\mathcal{M}}_{Ks}$. Then $h_{KK}:=\{h_s\}_{s\geqslant 0}$ and $g^0_{KK'}:=\{g^0_{KK's}\}_{s\geqslant 0}$ are compatible systems and, by propositions 3.3 and 5.9, they are special admisible locally analytic systems. By proposition 3.4 there is an $\eta_{KK'}\in\mathrm{Iso}^0(K,K')$ such that $g^0_{KK'\mathrm{an}}=\mathrm{d}(\eta_{KK'})\hat{\otimes}_k k(p)$. Notice also that if $\bar{n}_{KK'}:=\varprojlim_s n_s\in\varprojlim_s \mathbb{Z}/N_s\mathbb{Z}$ then $g_{KK'}=g^0_{KK'}\mathrm{Fr}(t_{K'})^{-\bar{n}_{KK'}*}$, where $\mathrm{Fr}(t_{K'})^*=\{\mathrm{Fr}(t_{K'})_s\}_{s\geqslant 0}$ is the compatible system from Subsection 3.5.

Suppose L is a finite Galois extension of E in $E(p)$ containing K. Proceed similarly to obtain $L'\subset E(p)$ such that g induces an isomorphism of $\Gamma_L(p)$ and $\Gamma_{L'}(p)$, the corresponding compatible system $g_{LL'}=\{g_{LL's}\}_{s\geqslant 0}$ and the special admissible locally analytic system $g^0_{LL'}=\{g^0_{LL's}\}_{s\geqslant 0}$, where $g_{LL'}=g^0_{LL'}\mathrm{Fr}(t_{L'})^{-\bar{n}_{LL'}*}$, together with the corresponding $\eta_{LL'}\in\mathrm{Iso}^0(L,L')$ such that $g^0_{LL'\mathrm{an}}=\mathrm{d}(\eta_{LL'})\hat{\otimes}_{k_L}k_L(p)$. Here k_L is the residue field of L, $k_L\simeq\mathbb{F}_{p^{M_0}}$ and $\bar{n}_{LL'}\in\varprojlim\mathbb{Z}/p^{M_0p^s}\mathbb{Z}$. Notice that all these maps depend on some choice of uniformising elements t_L and $t_{L'}$ in, respectively, L and L'.

The systems $g_{LL'}$ and $g_{KK'}$ are comparable because both come from the group isomorphisms $\Gamma_L(p)\longrightarrow\Gamma_{L'}(p)$ and $\Gamma_K(p)\longrightarrow\Gamma_{K'}(p)$ which are induced by g. If $I_{L/K}$ is the inertia subgroup of $\mathrm{Gal}(L/K)$ then there is a natural group embedding $I_{L/K}\subset\mathrm{Aut}^0(L)\subset\mathrm{Aut}^0(L_{\mathrm{ur}})$. Similarly, we have a group embedding for the inertia subgroup $I_{L'/K'}$ of $\mathrm{Gal}(L'/K')$ into $\mathrm{Aut}^0(L')$.

Let $\kappa: I_{L/K}\longrightarrow I_{L'/K'}$ be the group isomorphism induced by g. Then $\tau^*g_{LL's}=g_{LL's}\kappa(\tau)^*$, for any $\tau\in I_{L/K}$ and any $s\geqslant 0$. This implies that

$$\tau^*g_{LL'\mathrm{ur}}=g_{LL'\mathrm{ur}}\kappa(\tau)^*,$$

i.e. condition C from Subsection 3.7 holds in this case.

Let $\mu_{KK'}=\eta_{KK'}\mathrm{Fr}(t_{K'})^{-\bar{n}_{KK'}}\in\mathrm{Iso}(K,K')$ and $\mu_{LL'}=\eta_{LL'}\mathrm{Fr}(t_{K'})^{-\bar{n}_{LL'}}\in\mathrm{Iso}(L,L')$.

Proposition 6.1. *With the above notation:*
a) $\mu_{LL'}|_K=\mu_{KK'}$*;*
b) *for any* $\tau\in I_{L/K}$*,* $\tau\mu_{LL'}=\mu_{LL'}\kappa(\tau)$*.*

Proof. Let $\alpha=\mathrm{Fr}(t_{L'})^{\bar{n}_{LL'}}$. Consider K'_{ur} as a subfield in L'_{ur} and set $K''_{\mathrm{ur}}=\alpha(K'_{\mathrm{ur}})\subset L'_{\mathrm{ur}}$. Then K''_{ur} is the maximal unramified p-extension of the complete discrete valuation field $K'':=\alpha(K')\subset E(p)$ in $E(p)$.

Let $\beta=\alpha|_{K'_{\mathrm{ur}}}$. Consider the following commutative diagram

$$\begin{array}{ccccc}
\bar{\mathcal{M}}_{L\mathrm{ur}} & \xrightarrow{g_{LL'\mathrm{ur}}} & \bar{\mathcal{M}}_{L'\mathrm{ur}} & \xrightarrow{\alpha^*_{L'L'\mathrm{ur}}} & \bar{\mathcal{M}}_{L'\mathrm{ur}} \\
\downarrow & & \downarrow & & \downarrow \\
\bar{\mathcal{M}}_{K\mathrm{ur}} & \xrightarrow{g_{KK'\mathrm{ur}}} & \bar{\mathcal{M}}_{K'\mathrm{ur}} & \xrightarrow{\beta^*_{K'K''\mathrm{ur}}} & \bar{\mathcal{M}}_{K''\mathrm{ur}}
\end{array}$$

where the vertical arrows come from natural embeddings of the corresponding Galois groups.

The systems $g^0_{LL'}=g_{LL'}\alpha^*_{L'L'}$ and $f_{KK''}:=g_{KK'}\beta^*_{K'K''}$ are comparable, because they come from the compatible group isomorphisms $\Gamma_L(p)\longrightarrow\Gamma_{L'}(p)$ and $\Gamma_K(p)\xrightarrow{f}\Gamma_{K''}(p)$. In this situation, condition **C** is automatically satisfied and, by proposition 3.5, the admissibility of $g^0_{LL'}$ implies the admissibility of $f_{KK''}$. Because the group homomorphism f is compatible with ramification filtrations, we can apply the results of section 5 to deduce that $f_{KK''}$ is special admissible locally analytic and that there is an $\eta^1_{KK''}\in\mathrm{Iso}^0(K,K'')$ such that $f_{KK''\mathrm{an}}=\mathrm{d}(\eta^1_{KK''})\hat{\otimes}_k k(p)$ and $\eta_{LL'}|_K=\eta^1_{KK''}$.

Consider $\psi:=\eta^{-1}_{KK'}\eta_{LL'}|_K\in\mathrm{Iso}^0(K',K'')$. Then

$$\begin{aligned}\psi_{\mathrm{an}}&=\eta^{-1}_{KK'\mathrm{an}}\eta^1_{KK''\mathrm{an}}=(g^0_{KK'\mathrm{an}})^{-1}(g_{KK'}\beta^*_{K'K''})_{KK''\mathrm{an}}\\
&=\left({g^0_{KK'}}^{-1}g_{KK'}\beta^*_{K'K''}\right)_{K'K''\mathrm{an}}=\left(\mathrm{Fr}(t_{K'})^{-\bar{n}_{KK'}}\beta\right)_{\mathrm{an}}.\end{aligned}$$

Therefore by proposition 2.7,

$$\eta^{-1}_{KK'}\eta_{LL'}|_K=\mathrm{Fr}(t_{K'})^{-\bar{n}_{KK'}}\mathrm{Fr}(t_{L'})^{\bar{n}_{LL'}}|_K$$

or $\mu_{LL'}|_K=\mu_{KK'}$.

Part a) of our proposition is proved.

Consider the inertia subgroups $I_{L/K}\subset\mathrm{Gal}(L_{\mathrm{ur}}/K_{\mathrm{ur}})$, $I_{L'/K'}\subset\mathrm{Gal}(L'_{\mathrm{ur}}/K'_{\mathrm{ur}})$ and $I_{L'/K''}\subset\mathrm{Gal}(L'_{\mathrm{ur}}/K''_{\mathrm{ur}})$. As it was noticed earlier, the correspondence

$$\tau^*\mapsto\tau'^*=g^{-1}_{LL'\mathrm{ur}}\tau^*g_{LL'\mathrm{ur}}$$

induces a group isomorphism $\kappa:I_{L/K}\longrightarrow I_{L'/K'}$ such that $\kappa(\tau)=\tau'$.

We use the correspondence

$$\alpha^*:\tau'\mapsto\tau''=\alpha^{-1}\tau'\alpha$$

to define the group isomorphism $\kappa_\alpha:I_{L'/K'}\longrightarrow I_{L'/K''}$ such that $\kappa_\alpha(\tau')=\tau''$. With this notation we have the following equality of compatible systems

$$\tau^*_{LL}g^0_{LL'}=g^0_{LL'}{\tau''_{L'L'}}^*,$$

where as earlier, $g^0_{LL'}=g_{LL'}\alpha^*_{L'L'}$.

Therefore, the equality $(\tau\eta_{LL'})_{\mathrm{an}} = (\tau^*_{LL}g^0_{LL'})_{\mathrm{an}} = (g^0_{LL'}{\tau''_{L'L'}}^*)_{\mathrm{an}} = (\eta_{LL'}\tau'')_{\mathrm{an}}$ together with proposition 2.7 and the definition of τ'' imply that $\tau\eta_{LL'} = \eta_{LL'}\tau'' = \eta_{LL'}\alpha^{-1}\tau'\alpha$, i.e. $\tau\mu_{LL'} = \mu_{LL'}\tau'$.

The proposition is proved. $\square$

Let $\mu := \varinjlim \mu_{KK'} : E(p) \longrightarrow E(p)$. Clearly, it is a continuous field isomorphism and $\mu(E) = E'$.

Proposition 6.2. $\mu^* = g$.

Proof. As earlier, let K and K' be Galois extensions of E and E', respectively, such that $g(\Gamma_K(p)) = \Gamma_{K'}(p)$.

By part b) of the above proposition 6.1, the correspondences $\mu^* : \tau \mapsto \mu^{-1}\tau\mu$ and $g : \tau \mapsto g(\tau)$ induce the same isomorphism of the inertia subgroups $I_K(p) \longrightarrow I_{K'}(p)$. Consider the induced isomorphism $I_K(p)^{\mathrm{ab}} \longrightarrow I_{K'}(p)^{\mathrm{ab}}$. With respect to the identifications of class field theory $I_K(p)^{\mathrm{ab}} = U_K$ and $I_{K'}(p)^{\mathrm{ab}} = U_{K'}$, where U_K and $U_{K'}$ are groups of principal units in K and K', respectively, this homomorphism is induced by the restriction of the field isomorphism $\mu_{KK'}$ on U_K. In addition, $\mu_{KK'}$ transforms the natural action of any $\tau \in \Gamma_E(p)$ on U_K into the natural action of $g(\tau) \in \Gamma_{E'}(p)$ on $U_{K'}$. Therefore, the two field automorphisms $\mu^{-1}\tau\mu|_{K'}$ and $g(\tau)|_{K'}$ of K' become equal after restricting on $U_{K'}$. This implies that they coincide on the whole field K', i.e. $\mu^{-1}\tau\mu \equiv g(\tau) \bmod \Gamma_{K'}(p)$, for any $\tau \in \Gamma_E(p)$. Because K is an arbitrary Galois extension of E in $E(p)$ this implies that $g = \mu^*$.

So, proposition 6.2 together with the characteristic p case of the Main Theorem are completely proved. $\square$

7. Proof of the main theorem — the mixed characteristic case

In this section we assume that E is a field of characteristic 0. Clearly, this implies that the field E' is also of charactersitic 0.

7.1. Following the paper [10] introduce the categories Ψ, $\widetilde{\Psi}$ and the functor $\Phi : \Psi \longrightarrow \widetilde{\Psi}$.

The objects of Ψ are the field extensions L/K, where $[K : \mathbb{Q}_p] < \infty$, L is an infinite Galois extension of K in a fixed maximal p-extension $K(p)$ of K and $\Gamma_{L/K} = \mathrm{Gal}(L/K)$ is a p-adic Lie group. A morphism from L/K to an object L'/K' in Ψ is a continuous field embedding $f : L \longrightarrow L'$ such that $[L' : f(L)] < \infty$ and $f|_K$ is a field isomorphism of K and K'.

The objects of $\widetilde{\Psi}$ are couples $(\mathcal{K}, G)$ where $\mathcal{K}$ is a complete discrete valuation field of characteristic p with finite residue field and G is a closed subgroup of the group of all continuous automorphisms of $\mathcal{K}$. In addition, with respect to the induced topology G, is a compact finite dimensional

p-adic Lie group. A morphism from $(\mathcal{K}, G)$ to an object $(\mathcal{K}', G')$ in $\widetilde{\Psi}$ is a closed field embedding $f : \mathcal{K} \longrightarrow \mathcal{K}'$ such that $\mathcal{K}'$ is a finite separable extension of $f(\mathcal{K})$. In addition, $f(\mathcal{K})$ is G'-invariant and the corrspondence $\tau \mapsto \tau|_{f(\mathcal{K})}$ induces a group epimorphism from G' to G.

Let X be the Fontaine-Wintenberger field-of-norm functor, cf. [11]. Then the correspondence $L/K \mapsto (X(L), G_{L/K})$, where $G_{L/K} = \{X(\tau) \mid \tau \in \Gamma_{L/K}\}$, induces the functor $\Phi : \Psi \longrightarrow \widetilde{\Psi}$.

One of main results in [10] states that the functor Φ is fully faithful.

7.2. Let $\{E_\alpha/E, i_{\alpha\beta}\}_{\mathcal{I}}$ be an inductive system of objects in the category Ψ. From now on $\mathcal{I}$ is a set of indices α with a suitable partial ordering. The connecting morphisms $i_{\alpha\beta} \in \mathrm{Hom}_\Psi(E_\alpha, E_\beta)$ are the natural field embeddings defined for suitable couples $\alpha, \beta \in \mathcal{I}$. We can choose this inductive system to be large enough to satisfy the requirement $\varinjlim E_\alpha = E(p)$.

By applying the functor Φ, we obtain the inductive system $\{(\mathcal{E}_\alpha, G_\alpha), \tilde{i}_{\alpha\beta}\}_{\mathcal{I}}$ in the category $\widetilde{\Psi}$, where $(\mathcal{E}_\alpha, G_\alpha) = \Phi(E_\alpha/E)$ and $\tilde{i}_{\alpha\beta} = \Phi(i_{\alpha\beta})$, for all $\alpha \in \mathcal{I}$. Then $\varinjlim \mathcal{E}_\alpha = \mathcal{E}(p)$ is a maximal p-extension for each field $\mathcal{E}_\alpha$, $\alpha \in \mathcal{I}$.

Notice that the field embeddings $\tilde{i}_{\alpha\beta}$ induce group epimorphisms $\tilde{j}_{\alpha\beta} : G_\beta \longrightarrow G_\alpha$ with corresponding projective system $\{G_\alpha, \tilde{j}_{\alpha\beta}\}_{\mathcal{I}}$ such that $\varprojlim G_\alpha$ is identified via the functor X with $\Gamma_E(p)$. For any $\alpha \in \mathcal{I}$, we then have the identifications $\Gamma_{E_\alpha}(p) = \Gamma_{\mathcal{E}_\alpha}(p)$. These identifications are compatible with the ramification filtrations. This means that one can define the Herbrand function φ_α for the infinite extension E_α/E as the limit of Herbrand functions of all finite subextensions in E_α over E and

$$\Gamma_E(p)^{(v)} \cap \Gamma_{E_\alpha}(p) = \Gamma_{\mathcal{E}_\alpha}(p)^{(\varphi_\alpha(v))},$$

for all $v \geqslant 0$.

7.3. Consider the group isomorphism $g : \Gamma_E(p) \longrightarrow \Gamma_{E'}(p)$ from the statement of the Theorem. For $\alpha \in \mathcal{I}$, let $E'_\alpha \subset E'(p)$ be such that $g(\Gamma_{E_\alpha}(p)) = \Gamma_{E'_\alpha}(p)$. Then we have the corresponding injective system $\{E'_\alpha, i'_{\alpha\beta}\}_{\mathcal{I}}$ and $\varinjlim E'_\alpha = E'(p)$.

Clearly, for any $\alpha \in \mathcal{I}$,

- E'_α/E' is an object of Ψ;
- $\bar{g}_\alpha := g_\alpha \bmod \Gamma_{E_\alpha}(p) : \Gamma_{E_\alpha/E} \longrightarrow \Gamma_{E'_\alpha/E'}$ is a group isomorphism which is compatible with the ramification filtrations; in particular, this implies that the Herbrand functions for the infinite extensions E_α/E and E'_α/E' are equal;
- for any $v \geqslant 0$, $g_\alpha := g|_{\Gamma_{E_\alpha}(p)}$ induces a continuous group isomorphism of $\Gamma_E(p)^{(v)} \cap \Gamma_{E_\alpha}(p)$ and $\Gamma_{E'}(p)^{(v)} \cap \Gamma_{E'_\alpha}(p)$.

For $\alpha \in \mathcal{I}$, set $\Phi(E'_\alpha/E') = (\mathcal{E}'_\alpha, G'_\alpha)$ and $\Phi(i'_{\alpha\beta}) = \tilde{\imath}'_{\alpha\beta}$. Then we have an inductive system $\{(\mathcal{E}'_\alpha, G'_\alpha), \tilde{\imath}'_{\alpha\beta}\}_{\mathcal{I}}$ and $\varinjlim \mathcal{E}'_\alpha := \mathcal{E}'(p)$ is a maximal p-extension for each $\mathcal{E}'_\alpha$. As earlier, we obtain the projective system $\{G'_\alpha, \tilde{\jmath}'_{\alpha\beta}\}_{\mathcal{I}}$ and the field-of-norms functor allows us to identify the topological groups $\varprojlim G'_\alpha$ and $\Gamma_{E'}(p)$. Therefore, for any $\alpha \in \mathcal{I}$, we have an identification of the groups $\Gamma_{E'_\alpha}(p)$ and $\Gamma_{\mathcal{E}'_\alpha}(p)$.

This implies that for all $\alpha \in \mathcal{I}$, we have the following isomorphisms of topological groups:

- $\tilde{g}_\alpha := X(g_\alpha) : \Gamma_{\mathcal{E}_\alpha}(p) \longrightarrow \Gamma_{\mathcal{E}'_\alpha}(p)$ such that, for any rational number $v \geqslant 0$, $\tilde{g}_\alpha(\Gamma_{\mathcal{E}_\alpha}(p)^{(v)}) = \Gamma_{\mathcal{E}'_\alpha}(p)^{(v)}$;
- $X(\bar{g}_\alpha) : G_\alpha \longrightarrow G'_\alpha$ which maps the projective system $\{G_\alpha, \tilde{\jmath}_{\alpha\beta}\}_{\mathcal{I}}$ to the projective system $\{G'_\alpha, \tilde{\jmath}'_{\alpha\beta}\}_{\mathcal{I}}$.

7.4. By the characteristic p case of the Main Theorem for all $\alpha \in \mathcal{I}$, there are continuous field isomorphisms $\tilde{\mu}_\alpha : \mathcal{E}_\alpha \longrightarrow \mathcal{E}'_\alpha$ such that

- $\{\tilde{\mu}_\alpha\}_{\alpha\in\mathcal{I}}$ maps the inductive system $\{\mathcal{E}_\alpha, \tilde{\imath}_{\alpha\beta}\}_{\mathcal{I}}$ to the inductive system $\{\mathcal{E}'_\alpha, \tilde{\imath}'_{\alpha\beta}\}_{\mathcal{I}}$;
- $X(\bar{g}_\alpha)$ is induced by $\tilde{\mu}_\alpha$, i.e. if $\tau \in G_\alpha$ and $\tau' = X(\bar{g}_\alpha) \in G'_\alpha$ then $\tau\tilde{\mu}_\alpha = \tilde{\mu}_\alpha\tau'$.

Because Φ is a fully faithful functor, for all indices $\alpha \in \mathcal{I}$, there is a $\mu_\alpha \in \mathrm{Hom}_\Psi(E_\alpha/E, E'_\alpha/E')$ such that

- $\{\mu_\alpha\}_{\alpha\in\mathcal{I}}$ transforms the inductive system $\{E_\alpha/E, i_{\alpha\beta}\}_{\mathcal{I}}$ into the inductive system $\{E'_\alpha/E', i'_{\alpha\beta}\}_{\mathcal{I}}$;
- if $\tau \in \Gamma_{E_\alpha/E}$ and $\tau' = \bar{g}_\alpha(\tau) \in \Gamma_{E'_\alpha/E'}$ then $\tau\mu_\alpha = \mu_\alpha\tau'$.

Therefore, $\mu := \varinjlim \mu_\alpha$ is a continuous field isomorphism from $E(p)$ to $E'(p)$ such that $\tau\mu = \mu g(\tau)$, i.e. $g(\tau) = \mu^{-1}\tau\mu$, for $\tau \in \varprojlim \Gamma_{E_\alpha/E} = \Gamma_E(p)$ and $g(\tau) \in \varprojlim \Gamma_{E'_\alpha/E'} = \Gamma_{E'}(p)$.

The Main Theorem is completely proved.

References

[1] V.A. Abrashkin, *Ramification filtration of the Galois group of a local field. II.* Proceeding of Steklov Math. Inst. **208** (1995), 18–69.

[2] V.A. Abrashkin, *Ramification filtration of the Galois group of a local field. III.* Izvestiya RAN, ser. math. **62** (1998), 3–48.

[3] V.A. Abrashkin, *A local analogue of the Grothendieck conjecture.* Int. J. of Math. **11** (2000), 3–43.

[4] P. Berthelot, W. Messing, *Théorie de Deudonné Cristalline III: Théorèmes d'Équivalence et de Pleine Fidélité.* The Grotendieck Festschrift. A Collection of Articles Written in Honor of 60th Birthday of Alexander Grothendieck, volume 1, eds P.Cartier etc. Birkhauser, 1990, 173–247.

[5] J.-M. FONTAINE, *Representations p-adiques des corps locaux (1-ere partie)*. The Grothendieck Festschrift. A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck, volume II, eds. P.Cartier etc. Birkhauser, 1990, 249–309.

[6] K. IWASAWA, *Local class field theory*. Oxford University Press, 1986

[7] SH.MOCHIZUKI, *A version of the Grothendieck conjecture for p-adic local fields*. Int. J. Math. **8** (1997), 499–506.

[8] J.-P.SERRE, *Lie algebras and Lie groups*. Lectures given at Harvard University. New-York-Amsterdam, Bevjamin, 1965.

[9] I.R. SHAFAREVICH. *A general reciprocity law (In Russian)*. Mat. Sbornik **26** (1950), 113–146; Engl. transl. in Amer. Math. Soc. Transl. Ser. 2, volume **2** (1956), 59–72.

[10] J.-P. WINTENBERGER, *Extensions abéliennes et groupes d'automorphismes de corps locaux*, C. R. Acad. Sc. Paris, Série A **290** (1980), 201–203.

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

Victor ABRASHKIN
Math Dept of Durham University
Sci Laboratories, South Road
DH7 7QR Durham, UK
E-mail: `victor.abrashkin@durham.ac.uk`
URL: `http://www.maths.dur.ac.uk/~dma0va/`