GROUP SCHEMES OF PERIOD $p > 2$

Victor Abrashkin[1]

Abstract. For a prime number $p > 2$, we give a direct proof of Breuil's classification of finite flat group schemes killed by p over the valuation ring of a p-adic field with perfect residue field. As application we establish a correspondence between finite flat group schemes and Faltings's strict modules which respects associated Galois modules via the Fontaine-Wintenberger field-of-norms functor

0. Introduction.

Let p be a prime number and let k be a perfect field of characteristic p. Denote by K_{00} the fraction field of the ring of Witt vectors with coefficients in k. Let K_0 be a totally ramified field extension of K_{00} of degree e and let O_0 be the valuation ring of K_0. Let Gr'_{O_0} be the category of finite flat commutative p-group schemes G (i.e. the order $|G|$ of G is an integral power of p) over O_0. We shall use the notation Gr_{O_0} for the full subcategory in Gr'_{O_0} consisting of group schemes killed by p (i.e. such that $p\,\mathrm{id}_G = 0$). All further notation from this introduction will be carefully reminded in due course in the main body of the paper.

0.1 *Motivation.*

There were various approaches to the problem of description of the category Gr'_{O_0}; especially should be mentioned [Fo2] in the case $e = 1$, [Co] in the case $e < p - 1$, [Br1] and [Ki1-3] in the case of arbitrary e (everywhere results are not complete if $p = 2$). In all these cases the classification of group schemes appears in terms of categories of filtered modules and was deduced from the corresponding classification of p-divisible groups. More precisely, the case $e < p-1$ was treated in [Co] via Fontaine's results about p-divisible groups [Fo1] and the case of arbitrary e uses essentially either in [Br1] and [Ki1] the crystalline Dieudonne theory from [BBM], or in [Ki3] the Fontaine-Messing theory, or in [Ki2] the Zink theory of "displays and windows" [Zi].

On the other hand, there is an alternative approach resulted in an explicit description of algebras of group schemes together with the corresponding coalgebra structures. On the first place one should mention two classical papers [TO] and [Ra]. They give (in the case of the basic ring O_0) an explicit description of all simple objects of the category Gr'_{O_0} ($\equiv$ simple objects of Gr_{O_0}). For small e, the author disseminated these results to the whole category Gr_{O_0}, cf. [Ab2] for the case $e = 1$ and [Ab3] for the case $e \leqslant p - 1$. It is worth mentioning that: a) the

---

1991 *Mathematics Subject Classification.* 14L15, 11G09.

Key words and phrases. group schemes.

[1]Partially supported by EPSRC, GR/S72252/01

case $p = 2$ is studied completely in [Ab2]; b) under the assumption $e < p - 1$ all constructions in [Ab3] become extremely simple and require, as a matter of fact, only the knowledge of the classical Dieudonne theory of group schemes over perfect field of characteristic p.

Notice that the problem of alternative and direct description of objects of Gr'_{O_0} (and especialy of Gr_{O_0}) in the case of arbitrary e was considered in [Br2]. The reason is that Breuil's description of Gr'_{O_0} in [Br1] appears in a very elegant and natural way in terms of crystalline sheaves but in the very end all crystalline concepts can be successfully eliminated. Such simplified interpretation of the classification of p-divisible groups and finite flat group schemes was suggested in [Br2] and achieved in different ways in [Ki1-3]. Notice also that it is rather easy to construct and to prove the full faithfulness of the functor from an appropriate category of filtered modules to the category of finite flat group schemes. The main problem appears when proving that this functor is essentially surjective. This is where the crystalline (resp. the usual) Dieudonne theory plays a crucial role in [Br1] (resp. [Ab2,3]). Despite of the beauty and conceptuality of the crystalline Dieudonne theory this looks like a very long way around and it would be very interesting to understand what are the properties of finite flat group schemes we do need to establish this surjectivity. (These properties should be implicitly hidden in the crystalline Dieudonne theory.) Mention also that the surjectivity on the level of group schemes killed by p implies immediately the surjectivity for the whole category of p-group schemes and for many applications, e.g. [BCDT], we do need the knowledge of a complete classification of group schemes only on the level of objects killed by p.

In this paper we extend the approach from [Ab2,3] to the whole category Gr_{O_0} with no restrictions on e. The basic idea can be explained as follows. Suppose $G_0 = \operatorname{Spec} A_0 \in \mathrm{Gr}_{O_0}$. Then one can use the methods from [Ab2,3] (and to some extent from [Ab1]) if there are sufficiently many functions $a \in A_0$ such that for any $g_1, g_2 \in G_0(\bar{K})$,

$$a(g_1 + g_2) \equiv a(g_1) + a(g_2) \bmod p\bar{O}. \tag{0.1.1}$$

(Here $\bar{K}$ is an algebraic closure of K_0 and $\bar{O}$ is the valuation ring of $\bar{K}$.) Notice that if $e \leqslant p - 1$ then these functions appear just from the classical Dieudonne module $M(\bar{G}_0)$ of $\bar{G}_0 = G_0 \otimes k = \operatorname{Spec} \bar{A}_0$. (In this case the elements of $M(\bar{G}_0)$ appear as covectors $(a_{-n})_{n \geqslant 0} \in \mathrm{CW}(\bar{A}_0)$ and their zero components $a_0 \in \bar{A}_0$ give rise to such functions.) In the case of arbitrary e such functions generally do not exist (the example comes easily from extensions of the etale constant group scheme of order p via the multiplicative constant group scheme of order p) but they do appear if we pass to the extension of scalars $G_0 \otimes_{O_0} O$, where O is the valuation ring of $K = K_0(\pi)$ and $\pi^p = \pi_0$ is a uniformising element of K_0. This corresponds to the fact that the crystalline Dieudonne theory for $G_0 \otimes (O_0/p)$ provides not just a Dieudonne module but a sheaf of Dieudonne modules in the $fppf$ (or rather syntomic) topology and this sheaf is not generated by its global sections. Vice versa, we start with a suitable Breuil's category of filtered modules MF^e_S, cf. the definition below, and apply the methods from [Ab2,3] to construct the functor $\mathcal{G}_O : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}_O$. If $G = \operatorname{Spec} A \in \operatorname{Im} \mathcal{G}_O$ then the O-algebra A contains sufficiently many functions satisfying above condition (0.1.1) and (the author studied this from [Br1]) such group scheme G appears as extension of scalars of a unique $G_0 \in \mathrm{Gr}_{O_0}$. Finally, it remains to prove that for any $G_0 \in \mathrm{Gr}_{O_0}$, the

corresponding $G = G_0 \otimes_{O_0} O$ belongs to the image of the functor $\mathcal{G}_O$. This is the most difficult part of the paper, where the methods from [Ab1] were very helpful. This part can be considered as a replacement of crystalline Dieudonne theory in the context of group schemes over O_0 which are killed by p.

The interrelation between Gr_{O_0} and the image $\mathrm{Im}\,\mathcal{G}_O \subset \mathrm{Gr}_O$ can be illustrated by the following example. Consider the group $\mathrm{Ext}_{\mathrm{Gr}_{O_0}}((\mathbb{Z}/p)_{O_0}, \mu_{p,O_0})$ of extensions of the constant etale group scheme $(\mathbb{Z}/p)_{O_0}$ via the constant multiplicative group scheme μ_{p,O_0} in Gr_{O_0}. This group of extensions is naturally isomorphic to O_0^*/O_0^{*p}. The image of $\mathcal{G}_O$ gives only the subgroup

$$(1+pO)^\times/(O^{*p} \cap (1+pO)^\times) \subset O^*/O^{*p} \simeq \mathrm{Ext}_{\mathrm{Gr}_O}((\mathbb{Z}/p)_O, \mu_{p,O}).$$

But the embedding $O_0 \subset O$ induces the group isomorphism

$$O_0^*/O_0^{*p} \simeq (1+pO)^\times/(O^{*p} \cap (1+pO)^\times).$$

In addition, the fact that the multiplicative structure on $(1+pO)^\times$ can be transformed into additive structure on pO via the p-adic logarithm explains why the additive filtered modules are very helpful to describe the structure of $G_0 \otimes_{O_0} O$ but can't be used directly for $G_0 \in \mathrm{Gr}_{O_0}$.

We must notice that our strategy should work for all prime numbers p, but in this paper we consider only the case $p > 2$. The case $p = 2$ requires much more careful calculations and the author has not yet checked all details. But having in mind the results from [Ab2] one can expect in the case $p = 2$ the classification will be obtained for a slightly different category $\mathrm{Gr}^*_{O_0}$ under the additional assumption that k is algebraicly closed. The category $\mathrm{Gr}^*_{O_0}$ contains the same objects as Gr_{O_0} but the morphisms of this category come from the morphisms $G_1 \longrightarrow G_2$ in Gr_{O_0} modulo those which factor through the canonical projection to the maximal etale quotient $G_1 \longrightarrow G_1^{et}$ and the embedding of the maximal multiplicative subobject $G_2^m \longrightarrow G_2$.

0.2 *The main statement.*

As earlier, $O = O_K$, where $K = K_0(\pi)$, $\pi^p = \pi_0$ is a uniformising element in K_0. Suppose $S = k[[t]]$ and $\sigma : S \longrightarrow S$ is such that $\sigma(s) = s^p$ for any $s \in S$. Fix a ring identification $\kappa_{SO} : S/t^{ep}S \longrightarrow O/pO$ such that $\kappa_{SO}|k = \mathrm{id}$.

Let $\mathcal{MF}_S$ be the category of triples (M^0, M^1, φ_1), where M^0 is an S-module, M^1 is its submodule and $\varphi_1 : M^1 \longrightarrow M^0$ is a σ-linear morphism. The morphisms in this category are morphisms of filtered S-modules which commute with the corresponding φ_1's. By MF^e_S we denote the full subcategory in $\mathcal{MF}_S$ consisting of (M^0, M^1, φ_1) such that M^0 is a free S-module of finite rank, $M^1 \supset t^e M^0$ and $\varphi_1(M^1)S = M^0$.

Our main result is the following

Theorem. *There is an antiequivalence of categories* $\mathcal{G}^O_{O_0} : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}_{O_0}$.

Notice that this antiequivalence essentially depends on the choice of the field extension K of K_0 (the ring identification κ_{SO} is introduced just for technical reasons). It would be very interesting to understand how $\mathcal{G}^O_{O_0}$ depends on the choice of K. It is worth mentioning that $\mathcal{G}^O_{O_0}$ coincides with the restriction of Breuil's antiequivalence to the category Gr_{O_0}, cf. Section 8, but in our approach

the construction of this antiequivalence is quite direct and explicit and all proofs are given entirely in the limits of the theory of finite flat group schemes.

The above Theorem is proved in first 7 sections.

In Section 1 we introduce the category MF_S^e and explain that it is equivalent to the category of filtered S_0-modules with slope $\leqslant e$, where $S_0 = k[[t^p]] \subset S$. Then we introduce the concept of a φ_1-nilpotent lift of objects of $\mathcal{MF}_S$ to MF_S^e. It is related to the situation, where the knowledge of a quotient $\mathcal{N} \in \mathcal{MF}_S$ of $\mathcal{M} \in \mathrm{MF}_S^e$ is sufficient for a unique recovering of $\mathcal{M}$ from $\mathcal{N}$. As a matter of fact, this is the only idea from crystalline cohomology which survives in our setting.

In Section 2 we construct the functor $\mathcal{G}_O : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_O$ by applying directly the ideas from [Ab2,3]. For each $\mathcal{M} \in \mathrm{MF}_S^e$ we construct a family of explicitly given O-algebras $\mathcal{A}(\mathcal{M})$, for any $A \in \mathcal{A}(\mathcal{M})$ provide $G = \operatorname{Spec} A$ with a structure of an object of the category Gr_O and prove that all these G's are naturally isomorphic. A special case of algebras from $\mathcal{A}(\mathcal{M})$ plays a very important role in Sections 3 and 6 (it appears also in Breuil's paper [Br1, Section 3.1]), but in Sections 4 and 7 we do need more general algebras from $\mathcal{A}(\mathcal{M})$.

In Section 3 we prove that $\mathcal{G}_O$ is fully faithful. Namely, suppose $\mathcal{M} \in \mathrm{MF}_S^e$ and $G = \mathcal{G}_O(\mathcal{M}) = \operatorname{Spec} A$. Then $\mathcal{M}$ can be recovered uniquely as a φ_1-nilpotent lift of the following object $\mathcal{N}$ of the category $\mathcal{MF}_S$. Suppose $e_G : A \longrightarrow O$ and $\Delta_G : A \longrightarrow A \otimes A$ are the counit and the comultiplication of G. Set $I_A = \operatorname{Ker} e_G$, $I_{A\otimes A} = \operatorname{Ker} e_{G\times G}$ and $I_{A\otimes A}(p) = \{a \in I_{A\otimes A} \mid a^p \in pA \otimes A\}$. Introduce the ideal I_A^{DP} as the maximal ideal in I_A with the structure of nilpotent divided powers. (This means $a_0 \in I_A^{DP} \Leftrightarrow$ if for all $i \geqslant 0$, $a_{i+1} = -a_i^p/p$ then $a_i \to 0$ as $i \to \infty$.) Then $\mathcal{N} = (N^0, N^1, \varphi_1)$, where (compare with (0.1.1))

$$N^0 = \{a \in I_A \mid \Delta_G(a) \equiv a \otimes 1 + 1 \otimes a \bmod I_{A\otimes A}(p)^p\} \bmod I_A^{DP}, \tag{0.2.1}$$

$N^1 = (I_A(p)/I_A^{DP}) \bigcap N^0$ and φ_1 is induced by the correspondence $a \mapsto -a^p/p$ with $a \in I_A(p)$. As we have noticed earlier, we introduce here a special way to construct the O-algebras of group schemes $\mathcal{G}_O(\mathcal{M})$, $\mathcal{M} \in \mathrm{MF}_S^e$, and define for all $\alpha \in O$, the special ideals $I_A(\alpha)$ in A and $I_{A\otimes A}(\alpha)$ in $A \otimes A$. These technical notions will play an important role in Section 6.

In Section 4 we prove that one can study the image of $\mathcal{G}_O$ by replacing if necessary the ring O by the valuation ring of any tamely ramified extension of its fraction field K. In particular, this will allow us later to treat any $G \in \mathrm{Gr}_O$ as a result of successive extensions via group schemes of order p. We also prove in this section that any $G \in \mathcal{G}_O(\mathcal{M})$ comes via extension of scalars from a unique $G_0 \in Gr_{O_0}$.

In section 5 we describe torsors of group schemes of order p over flat O-algebras. As a matter of fact, this is a detailed revision of the corresponding result from [Ab1]. Then we use this description (again following the strategy from [Ab1]) to describe the group of extensions of $H \in \mathrm{Gr}_O$ via group schemes of order p in the category Gr_O. Notice that in this section we do not assume that O is obtained in the form $O_0[\pi]$, where $\pi^p = \pi_0$.

Section 6 contains the proof of the Main Lemma. This lemma is quite technical, the calculations are done in the spirit of [Ab1] but are based on a different background. As we have noticed earlier, this technical lemma provides us with the fact that $A(G_0)_{O_0} \otimes O$ contains sufficiently many functions satisfying condition (0.1.1), or equivalently, that the crystalline Dieudonne sheaf associated with G_0 contains sufficiently many sections over O.

Finally, in Section 7 we apply the results of previous Sections 4-6 to deduce that for any $G_0 \in Gr_{O_0}$, its extension of scalars $G = G_0 \otimes_{O_0} O$ belongs to the image of the functor $\mathcal{G}_O$. This gives the existence of a functor $\mathcal{G}^O_{O_0} : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}_{O_0}$ such that for any $\mathcal{M}$, $\mathcal{G}^O_{O_0}(\mathcal{M}) = G_0$, and the full faithfulness of $\mathcal{G}_O$ implies that $\mathcal{G}^O_{O_0}$ is an antiequivalence of categories.

In section 8 we give several applications of our methods. In particular, we prove that our antiequivalence coincides with the Breuil antiequivalence restricted to the category Gr_{O_0}. Luckily, when proving this compatibility it was possible to use a technical result about sections of Dieudonne crystalline sheaves from [Br1] to avoid diving into crystalline aspects of Breuil's theory. We also establish a criterion for $\mathbb{F}_p[\Gamma_{K_0}]$-modules to appear in the form $G_0(\bar{K})$, $G_0 \in \mathrm{Gr}_{O_0}$, and apply it to relate these modules to Galois modules of kernels of isogenies of Drinfeld modules via the field-of-norms functor, cf. Subsection 0.3 below for more commentaries. Finally, we establish the interpretation of the Cartier duality in Gr_{O_0} in terms of filtered modules from MF^e_S. The Cartier duality is described in terms of special algebras for $H = H_0 \otimes_{O_0} O$ and $\widetilde{H} = \widetilde{H}_0 \otimes_{O_0} O$, where $H_0, \widetilde{H}_0 \in \mathrm{Gr}_{O_0}$ and $\widetilde{H_0}$ is the Cartier dual to H_0, via an explicit construction of the corresponding non-degenerate bilinear pairing of group functors $H \times \widetilde{H} \longrightarrow \mu_{p,O}$.

0.3 *Relation to Faltings's strict modules.*

Let V be a finite $\mathbb{F}_p[\Gamma_K]$-module, where $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$. Introduce the object $T(V) = (T(V)^0, T(V)^1, \varphi_1)$ of the category $\mathcal{MF}_S$ such that $T(V)^0 = \mathrm{Hom}^{\Gamma_K}(V, \bar{O} \bmod p)$, $T(V)^1 = \{a \in T(V)^0 \mid a^p = 0\}$ and $\varphi_1 : T(V)^1 \longrightarrow T(V)^0$ is induced by the correspondences $o \mapsto -o^p/p$ where $o \in \bar{O}$.

In Section 8.2 we prove the following criterion:

(0.3.1). *Suppose $\mathcal{M} \in \mathrm{MF}^e_S$, $G = \mathcal{G}_O(\mathcal{M})$ and $|G(\bar{K})| = |V|$. Then the $\mathbb{F}_p[\Gamma_K]$-modules V and $G(\bar{K})$ are isomorphic if and only if in the category $\mathcal{MF}_S$ there is a φ_1-nilpotent morphism $\mathcal{M} \longrightarrow T(V)$.*

This criterion makes precise the fundamental role of functions satisfying condition (0.1.1). It also allows us to study the following problem. Remind that by Raynaud's theorem any finite flat commutative group scheme over O_0 arises as the kernel of an isogeny in the category Ab_{O_0} of abelian schemes over O_0. The characteristic p analogue of Ab_{O_0} is the category of Drinfeld modules $\mathrm{Dr}(S_{00})_{S_0}$ over S_0, where $S_{00} = \mathbb{F}_p[\tau_{00}] \subset S_0$ is such that $\mathcal{K}_{00} = \mathrm{Frac}\,\mathbb{F}_p[[\tau_{00}]]$ is a closed subfield in $\mathcal{K}_0 = \mathrm{Frac}\, S_0$ and the ramification index of $\mathcal{K}_0$ over $\mathcal{K}_{00}$ is e. The kernels of isogenies in $\mathrm{Dr}(S_{00})_{S_0}$ are analogs of classical group schemes. They can be introduced and studied directly as finite flat group schemes with strict action of S_{00}, cf. [Fa], [Ab4]. In this setting the characteristic p analog of Gr_{O_0} is the category $\mathrm{Gr}(S_{00})_{S_0}$ of finite flat commutative group schemes over S_0 with strict action of S_{00} which are killed by the action of τ_{00}. (In [Ab4] this category was denoted by $\mathrm{DGr}^{\prime *}_1(S_{00})_{S_0}$).

As a special case of the classification of strict modules from [Ab4] we have the antiequivalence $\mathcal{G}^S_{S_0} : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}(S_{00})_{S_0}$. (The category MF^e_S was denoted in [Ab4] by $\mathrm{BR}_1(S_{00})_{S_0}$.)

Suppose $\mathcal{M} \in \mathrm{MF}^e_S$, $H_0 = \mathcal{G}^O_{O_0}(\mathcal{M}) \in \mathrm{Gr}_{O_0}$ and $\mathcal{H}_0 = \mathcal{G}^S_{S_0}(\mathcal{M}) \in \mathrm{Gr}(S_{00})_{S_0}$.

Let $\bar{\mathcal{K}}$ be an algebraic closure of $\mathcal{K}_0$ and $\Gamma_{\mathcal{K}_0} = \mathrm{Aut}_{\mathcal{K}_0}(\bar{\mathcal{K}})$. As earlier, $\bar{K}$ is an algebraic closure of K and $\Gamma_{K_0} = \mathrm{Gal}(\bar{K}/K_0)$. Consider the Γ_{K_0}-module $V_0 = H_0(\bar{K})$ and the $\Gamma_{\mathcal{K}_0}$-module $\mathcal{V}_0 = \mathcal{H}_0(\bar{\mathcal{K}})$. (Notice that by [Ab4], $\mathcal{H}_0$ has an etale generic fibre.)

As an application of the above criterion (0.3.1) we show that the Galois modules V_0 and $\mathcal{V}_0$ can be identified via the Fontaine-Wintenberger functor field-of-norms. More precisely, consider the arithmetically profinite extension

$$K_\infty = K_0(\{\pi_n \mid \pi_1 = \pi, \pi_{n+1}^p = \pi_n\}).$$

Then the field-of-norms functor gives an identification of $\Gamma_{K_\infty} = \mathrm{Gal}(\bar{K}/K_\infty)$ and $\Gamma_{\mathcal{K}_0}$ and we have the following property:

(0.3.2). *With the above identification* $\Gamma_{\mathcal{K}_0} = \Gamma_{K_\infty}$*, it holds* $\mathcal{V}_0 \simeq V_0|_{\Gamma_{K_\infty}}$.

As a matter of fact, we can say more. Suppose $\Gamma_{K_0}(V_0) = \{\tau \in \Gamma_{K_0} \mid \tau|_{V_0} = \mathrm{id}\}$ and $\Gamma_{\mathcal{K}_0}(\mathcal{V}_0) = \{\tau \in \Gamma_{\mathcal{K}_0} \mid \tau|_{\mathcal{V}_0} = \mathrm{id}\}$. Then the embedding $\Gamma_{\mathcal{K}_0} = \Gamma_{K_\infty} \longrightarrow \Gamma_{K_0}$ induces a group isomorphism $\Gamma_{\mathcal{K}_0}/\Gamma_{\mathcal{K}_0}(\mathcal{V}_0) \simeq \Gamma_{K_0}/\Gamma_{K_0}(V_0)$. Therefore, the Galois modules $\mathcal{V}_0$ and V_0 can be uniquely recovered one from another. There are another situations where there is definitely similar relation between the kernels of isogenies of Drinfeld modules and the kernels of isogenies of abelian schemes. The study of this problem should be useful when studying the image of the functor $V \mapsto V|_{\Gamma_{\mathcal{K}_0}}$, where V is a "geometrically interesting" (e.g. crystalline, semistable) representation of Γ_{K_0}.

The above approach can be applied to the study of the functor from the category of finite flat $\mathbb{Z}_p[\Gamma_{K_0}]$-modules (i.e. the Galois modules of the form $G(\bar{K})$, where $G \in \mathrm{Gr}'_{O_0}$) to the category of Γ_{K_∞}-modules given by the restriction of Galois action to $\Gamma_{K_\infty} \subset \Gamma_{K_0}$. Our method allows to obtain Breuil's result, [Br4, Theorem 3.4.3], about full faithfulness of this functor just from Fontaine's ramification estimate: for all $v > ep/(p-1) - 1$, the ramification subgroups $\Gamma_{K_0}^{(v)}$ act trivially on $G_0(\bar{K})$, where $G_0 \in \mathrm{Gr}_{O_0}$. This idea also works in the context of finite subquotients of crystalline representations over unramified base with Hodge-Tate weights of length $< p$ by using the ramification estimate from [Ab5]. (The case of Hodge-Tate weights $\leqslant p-2$ was considered in [Br3] and can be retrieved even with Fontaine's ramification estimate from [Fo5].) We must mention here that recently Kisin [Ki3, Theorem 02] proved the full faithfulness of the functor $V \mapsto V|_{\Gamma_{K_\infty}}$ in the context of all crystalline $\mathbb{Q}_p[\Gamma_{K_0}]$-modules. (Everywhere in this paragraph p is any prime number.)

We shalll use without special reference the following notation:
Basic Notation.

- If A, B, C are sets and $f : A \longrightarrow B$, $g : B \longrightarrow C$ then their composition will be denoted by fg or, sometimes, by $f \circ g$.

- k is a perfect field of characteristic $p > 2$, K_{00} is the fraction field of the ring of Witt vectors $W(k)$, K_0 is a totally ramified extension of K_{00} of degree e with fixed uniformising element π_0 and the valuation ring O_0, $K = K_0(\pi)$ and $O = O_0[\pi]$, where $\pi^p = \pi_0$; $\bar{K}$ is a fixed algebraic closure of K, $\bar{O}$ is the valuation ring of $\bar{K}$, and for any field extension E of K_0 in $\bar{K}$, $\Gamma_E = \mathrm{Gal}(\bar{K}/E)$;

- Gr'_{O_0}, resp., Gr'_O, is the category of all finite flat p-group schemes over O_0, resp., O; Gr_{O_0} and Gr_O are the corresponding full subcategories consisting of objects killed by p; for any finite flat group scheme H we denote by $A(H)$, Δ_H and e_H, resp., the affine algebra, the comultiplicatiopn and the counut of H;

• In the category Aug_O of augmented O-algebras, I_A is always the augmentation ideal of $A \in \mathrm{Aug}_O$;

• $\phi(X,Y) = (X^p + Y^p - (X+Y)^p)/p \in \mathbb{Z}[X,Y]$ is the first Witt polynomial and $\phi(X)$ is just an abbreviation for $\phi(X \otimes 1, 1 \otimes X)$;

• for an indeterminate t, we set $S = k[[t]]$, $\sigma : S \longrightarrow S$ is the morphism of p-th power, $S_0 = k[[t_0]] \subset S$ with $t_0 = t^p$, the corresponding fraction fields are $\mathcal{K} = \mathrm{Frac}\, S$ and $\mathcal{K}_0 = \mathrm{Frac}\, S_0$; $\kappa_{SO} : S/t^{ep} \longrightarrow O/pO$ is a ring isomorphism such that $\kappa_{SO}(t) = \pi \bmod p$ and for any $\alpha \in k$, $\kappa_{SO}(\alpha) = [\alpha] \bmod p$, where $[\alpha]$ is the Teichmüller representative of α.

1. A category of filtered modules.

1.1. *The categories* MF_S^e *and* $\mathcal{MF}_S$.

Suppose $e \in \mathbb{N}$. Denote by MF_S^e the category of triples (M^0, M^1, φ_1), where M^0 is a free S-module of finite rank, $M^1 \subset M^0$ is a submodule such that $M^1 \supset t^e M^0$, and $\varphi_1 : M^1 \longrightarrow M^0$ is a σ-linear morphism of S-modules such that the set $\varphi_1(M^1)$ generates M^0 over S. Notice that M^1 is a free S module, $\mathrm{rk}_S M^0 = \mathrm{rk}_S M^1$, and φ_1 maps any S-basis of M^1 to an S-basis of M^0. The morphisms $(M^0, M^1, \varphi_1) \longrightarrow (M_1^0, M_1^1, \varphi_1)$ in MF_S^e are given by S-linear morphisms $f : M^0 \longrightarrow M_1^0$ such that $f(M^1) \subset M_1^1$ and $f\varphi_1 = \varphi_1 f$.

Let $S_0 = \sigma(S)$. Then $S_0 = k[[t_0]]$, where $t_0 = t^p$. Consider the category MF_{e,S_0} of S_0-modules with slope $\leqslant e$. Its objects are couples (M, φ), where M is a free S_0-module of finite rank, $\varphi : M^{(\sigma)} \longrightarrow M$, where $M^{(\sigma)} = M \otimes_{(S_0,\sigma)} S_0 \longrightarrow M$, is an S_0-linear morphism such that its image contains $t_0^e M$. The morphisms in MF_{e,S_0} are morphisms of the corresponding modules which commute with φ. The category MF_{e,S_0} is equivalent to MF_S^e. This equivalence can be given by the identification of rings $S_0 \otimes_{(S_0,\sigma)} S_0 = S$ (where $t_0 \otimes 1 \mapsto t$), the correspondence $(M, \varphi) \mapsto (M^{(\sigma)}, M^1, \varphi_1)$, where $M^1 = \varphi^{-1}(t_0^e M)$ and $\varphi_1 = t_0^{-e}\eta\varphi|_{M^1}$ with any fixed $\eta \in S^*$.

Introduce the category $\mathcal{MF}_S$ as the category of triples (M^0, M^1, φ_1), where M^0 is an S-module, M^1 is a submodule in M^0, and φ_1 is a σ-linear morphism from M^1 to M^0. The morphisms $f : (N^0, N^1, \varphi_1) \longrightarrow (M^0, M^1, \varphi_1)$ in $\mathcal{MF}_S$ are given by linear morphisms $f : N^0 \longrightarrow M^0$, such that $f(N^1) \subset M^1$ and $f\varphi_1 = \varphi_1 f$.

The category $\mathcal{MF}_S$ is additive, in particular, f is epimorphic iff $f(N^0) = M^0$. We shall call f *strictly epimorphic* if in addition $f(N^1) = M^1$.

Notice that MF_S^e is a full subcategory in $\mathcal{MF}_S$.

1.2 φ_1-*nilpotent lifts.*

Suppose $\mathcal{N} = (N^0, N^1, \varphi_1)$ and $\mathcal{M} = (M^0, M^1, \varphi_1)$ are objects of $\mathcal{MF}_S$ and $\theta \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}, \mathcal{M})$.

Definition. a) θ will be called φ_1-*nilpotent* if for $T = \ker\theta \subset N^0$, it holds $\mathrm{Ker}(\theta|_{N^1}) = T$, $\varphi_1(T) \subset T$ and $\varphi_1|_T$ is topologically nilpotent. (This means that if $T = T^{(0)}$ and for $i \geqslant 0$, $T^{(i+1)} = \varphi_1(T^{(i)})S$, then $\bigcap\limits_{i \geqslant 0} T^{(i)} = 0$.)

b) if $\mathcal{N} \in \mathrm{MF}_S^e$ and θ is strictly epimorphic and φ_1-nilpotent then we say that θ is *a* φ_1-*nilpotent lift* of $\mathcal{M}$ to MF_S^e.

Notice that the composition of φ_1-nilpotent lifts is again φ_1-nilpotent.

Proposition 1.2.1. *Suppose $\mathcal{M}, \mathcal{M}_1 \in \mathcal{MF}_S$ and $\theta_1 : \mathcal{N}_1 \longrightarrow \mathcal{M}_1$, $\theta : \mathcal{N} \longrightarrow \mathcal{M}$ are φ_1-nilpotent lifts to MF_S^e. Then for any $f \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}_1, \mathcal{M})$ there is a unique $\hat{f} \in \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{N}_1, \mathcal{N})$ such that $\hat{f}\theta = \theta_1 f$.*

Proof. The proof can be easily obtained from the following Lemma.

Lemma 1.2.2. *Suppose $\mathcal{N}, \mathcal{M} \in \mathcal{MF}_S$ and $\theta \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}, \mathcal{M})$ is φ_1-nilpotent and strictly epimorphic. Then for any $\mathcal{N}_1 \in \mathrm{MF}_S^e$, the map $\theta_* : \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}_1, \mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}_1, \mathcal{M})$ is bijective.*

Proof of Lemma. Let $\mathcal{N}_1 = (N_1^0, N_1^1, \varphi_1)$. Choose an S-basis $n_1^1, \ldots, n_u^1$ in N_1^1 and set $\bar{n}_1^1 = (n_1^1, \ldots, n_u^1)$. Let $\bar{n}_1 = \varphi_1(\bar{n}_1^1) := (n_1, \ldots, n_u)$, where for all $1 \leqslant i \leqslant u$, $n_i = \varphi_1(n_i^1)$. Then $n_1, \ldots, n_u$ is an S-basis of N_1^0 and there is a matrix $U \in M_u(S)$ such that $\bar{n}_1^1 = \bar{n}_1 U$. We shall use below a similar vector notation.

Suppose $\mathcal{N} = (N^0, N^1, \varphi_1)$, $\mathcal{M} = (M^0, M^1, \varphi_1)$ and $f \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}_1, \mathcal{M})$. Then f is uniquely given by two vectors $f(\bar{n}_1) = \bar{m}$ and $f(\bar{n}_1^1) = \bar{m}^1$ with coordinates in M^0 and M^1, resp., such that $\varphi_1(\bar{m}^1) = \bar{m}$ and $\bar{m}^1 = \bar{m}U$.

Choose a vector $\bar{n}^{(0)1}$ with coordinates in N^1 such that $\theta(\bar{n}^{(0)1}) = \bar{m}^1$ and set $\bar{n}^{(0)} = \varphi_1(\bar{n}^{(0)1})$. For $i \geqslant 0$, define by induction on i the vectors $\bar{n}^{(i)}$ and $\bar{n}^{(i)1}$ as follows: $\bar{n}^{(i+1)1} = \bar{n}^{(i)}U$ and $\varphi_1(\bar{n}^{(i+1)1}) = \bar{n}^{(i+1)}$.

Then the sequences $\{\bar{n}^{(i)1}\}_{i\geqslant 0}$ and $\{\bar{n}^{(i)}\}_{i\geqslant 0}$ converge in N^1 and, resp., N^0.

Indeed, use the submodules $T^{(i)}$, $i \geqslant 0$, in N^1 from the above definition of φ_1-nilpotent morphism π. Then $\bar{n}^{(0)1} - \bar{n}^{(1)1}$ has coordinates in $T = T^{(0)}$, its φ_1-image $\bar{n}^{(0)} - \bar{n}^{(1)}$ has coordinates in $\varphi_1(T^{(0)})$ and $\bar{n}^{(1)1} - \bar{n}^{(2)1}$ has coordinates in $\varphi_1(T^{(0)})S_1 = T^{(1)}$. Similarly, for any $i \geqslant 0$, $\bar{n}^{(i)} - \bar{n}^{(i+1)}$ and $\bar{n}^{(i)1} - \bar{n}^{(i+1)1}$ have coordinates in $T^{(i)}$. So, the condition $\bigcap\limits_{i\geqslant 0} T^{(i)} = 0$ implies that the both sequences are Cauchy and, therefore, converge.

Now let $\bar{n}^1 \in N^1$ and $\bar{n} \in N^0$ be limits of the above sequences $\{\bar{n}^{(i)1}\}_{i\geqslant 0}$ and $\{\bar{n}^{(i)}\}_{i\geqslant 0}$, resp. Then $\varphi_1(\bar{n}^1) = \bar{n}$ and $\bar{n}^1 = \bar{n}U$. So, the correspondences $\bar{n}_1^1 \mapsto \bar{n}^1$ and $\bar{n}_1 \mapsto \bar{n}$ define $g \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}_1, \mathcal{N})$. But $\theta(\bar{n}) = \bar{m}$ and $\pi(\bar{n}^1) = \bar{m}^1$ because for all $i \geqslant 0$, $\pi(\bar{n}^{(i)}) = \bar{m}$ and $\pi(\bar{n}^{(i)1}) = \bar{m}^1$. So, $f = \theta_*(g)$ and θ_* is surjective.

Suppose $g' \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{N}_1, \mathcal{N})$ is such that $\theta_*(g') = f$. Then $g'(\bar{n}_1) = \bar{n}'$ and, resp., $g'(\bar{n}_1^1) = \bar{n}'^1$ have coordinates in N^0 and N^1, resp. Notice also that $\varphi_1(\bar{n}'^1) = \bar{n}'$, $\bar{n}'^1 = \bar{n}'U$, $\theta(\bar{n}') = \bar{m}$ and $\theta(\bar{n}'^1) = \bar{m}^1$. Therefore, $\bar{n}'^1 - \bar{n}^{(0)1}$ has coordinates in $T^{(0)}$, $\bar{n}' - \bar{n}^{(0)}$ has coordinates in $\varphi_1(T^{(0)})$, $\bar{n}'^1 - \bar{n}^{(1)1}$ has coordinates in $\varphi_1(T^{(0)})S_1 = T^{(1)}$ and so on. In other words, for any $i \geqslant 0$, $\bar{n}'^1 - \bar{n}^{(i+1)1}$ and $\bar{n}' - \bar{n}^{(i)}$ have coordinates in $T^{(i)}$. Taking limits we obtain that $\bar{n}'^1 = \bar{n}^1$ and $\bar{n}' = \bar{n}$, i.e. $g = g'$.

The Lemma is proved. □

1.2.3. With notation from above Proposition 1.2.1, $\hat{f}$ will be called *a φ_1-nilpotent lift* of f. Notice also the following properties:

a) the correspondence $f \mapsto \hat{f}$ induces an injective homomorphism

$$\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}_1, \mathcal{M}) \longrightarrow \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{N}_1, \mathcal{N});$$

b) a φ_1-nilpotent lift is unique up to a unique isomorphism in MF_S^e; in particular, a φ_1-nilpotent lift of $\mathcal{M} \in \mathrm{MF}_S^e$ to MF_S^e is an isomorphism;

c) if $\mathcal{M} \in \mathcal{MF}_S$, $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}^e_S$ and $\theta : \mathcal{N} \longrightarrow \mathcal{M}$ is a φ_1-nilpotent lift of $\mathcal{M}$ then $\mathrm{Ker}\,\theta \subset tN^1$. (Indeed, if $n \in \mathrm{Ker}\,\theta$ and $n \notin tN^1$ then for any $i \geqslant 1$, $\varphi_1^i(n) \in N^1 \setminus tN^0$ and, therefore, does not converge to 0.)

1.3 *Simplest objects and their extensions.*

Let $\mathcal{M} = (M^0, M^1, \varphi_1)$, $\mathcal{M}_1 = (M_1^0, M_1^1, \varphi_1)$, $\mathcal{M}_2 = (M_2^0, M_2^1, \varphi_1)$ be objects of $\mathcal{MF}_S$. By definition, the sequence $0 \longrightarrow \mathcal{M}_1 \longrightarrow \mathcal{M} \longrightarrow \mathcal{M}_2 \longrightarrow 0$ is *short exact* in $\mathcal{MF}_S$ if the corresponding sequence of S-modules $0 \longrightarrow M_1^0 \longrightarrow M^0 \longrightarrow M_2^0 \longrightarrow 0$ and the induced sequence of maps of their submodules $0 \longrightarrow M_1^1 \longrightarrow M^1 \longrightarrow M_2^1 \longrightarrow 0$ are short exact. Then for given $\mathcal{M}_1, \mathcal{M}_2$, one can define, as usually, the set of classes of equivalence of short exact sequences $\mathrm{Ext}_{\mathcal{MF}_S}(\mathcal{M}_2, \mathcal{M}_1)$, and this set has a natural structure of abelian group.

Definition. If $\tilde{s} \in S$ is such that $\tilde{s}|t^e$ define the object $\mathcal{M}_{\tilde{s}}$ of MF^e_S as (Sm, Sm^1, φ_1) such that $\varphi_1(m^1) = m$ and $m^1 = \tilde{s}m$. Such objects $\mathcal{M}_{\tilde{s}}$ will be called *simplest*.

Remark 1.3.1. Notice that, if $\tilde{s}, \tilde{s}' \in S$ are divisors of t^e then $\mathcal{M}_{\tilde{s}} \simeq \mathcal{M}_{\tilde{s}'}$ iff $\tilde{s}' = \tilde{s}u^{p-1}$, where $u \in S^*$. In particular, by enlarging if necessary the residue field k we can always assume that $\tilde{s}$ is just an integral power of t.

Let $\mathcal{K}'$ be a finite field extension of $\mathcal{K} = \mathrm{Frac}\, S$ and let S' be the valuation ring of $\mathcal{K}'$. If e_0 is the ramification index of the field extension $\mathcal{K}'/\mathcal{K}$ and $e' = ee_0$ then there is a functor from MF^e_S to $\mathrm{MF}^{e'}_{S'}$ given by the extension of scalars $\mathcal{M} = (M^0, M^1, \varphi_1) \mapsto \mathcal{M} \otimes_S S' := (M^0 \otimes_S S', M^1 \otimes_S S', \varphi_1 \otimes_S S')$.

Proposition 1.3.2. *If $\mathcal{M} \in \mathrm{MF}^e_S$ then there is a tamely ramified extension $\mathcal{K}'/\mathcal{K}$ such that $\mathcal{M} \otimes_S S'$ can be obtained by a sequence of successive extensions via simplest objects of the category $\mathrm{MF}^{e'}_{S'}$.*

Proof. Let $\mathcal{M} = (M^0, M^1, \varphi_1)$. The embedding $M^1 \subset M^0$ induces the identification of $\mathcal{K}$-vector spaces $V := M^0 \otimes_S \mathcal{K} = M^1 \otimes_S \mathcal{K}$ and φ_1 induces a σ-linear morphism $\varphi_1 : V \longrightarrow V$ such that $\varphi_1(V)\mathcal{K} = V$. Therefore, V is an etale φ_1-module, cf. [Fo4], and we can apply the antiequivalence of the category of etale φ_1-modules and the category of continuous $\mathcal{K}[\Gamma_{\mathcal{K}}]$-modules H, where $\Gamma_{\mathcal{K}} = \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K})$, cf. [loc cit]. This antiequivalence is given by the correspondence

$$V \mapsto H := \{f \in \mathrm{Hom}_{\mathcal{K}}(V, \mathcal{K}_{\mathrm{sep}}) \mid \forall v \in V, f(\varphi_1(v)) = f(v)^p\}.$$

(Here $\Gamma_{\mathcal{K}}$ acts on H via its natural action on $\mathcal{K}_{\mathrm{sep}}$.) Notice that the inverse functor is induced by the correspondence $H \mapsto V = \mathrm{Hom}_{\mathcal{K}[\Gamma_{\mathcal{K}}]}(H, \mathcal{K}_{\mathrm{sep}})$.

Then use that the action of the wild inertia subgroup of $\Gamma_{\mathcal{K}}$ on H is unipotent. This implies the existence of a finite tamely ramified field extension $\mathcal{K}'$ of $\mathcal{K}$ such that $H \otimes_{\mathcal{K}} \mathcal{K}'$ has a decreasing filtration by its $\mathcal{K}'[\Gamma_{\mathcal{K}'}]$-submodules such that the corresponding quotients are 1-dimensional $\mathcal{K}'$-vector spaces with the trivial action of $\Gamma_{\mathcal{K}'}$. Therefore, $V \otimes_{\mathcal{K}} \mathcal{K}'$ has a $\mathcal{K}'$-basis $v_1, \ldots, v_u$ such that for all $1 \leqslant i \leqslant u$,

$$\varphi_1(v_i) = v_i + \sum_{j>i} v_j \alpha_{ji},\ \alpha_{ji} \in \mathcal{K}'.$$

Therefore, $M^1 \otimes_S S'$ has an S'-basis $m_1^1, \ldots, m_u^1$ such that for $1 \leqslant i \leqslant u$,

$$\varphi_1(m_i^1) = \sum_{j \geqslant i} m_j^1 u_{ji},\ u_{ji} \in S'.$$

It remains to notice that for $1 \leqslant i \leqslant u$, $m_i = \varphi_1(m_i^1)$ is an S'-basis of $M_{S'}^0 = M^0 \otimes_S S'$, and the condition $M^1 \supset t^e M^0$ implies that all $\tilde{s}_i := u_{ii}$ divide t^e. The proposition is proved. $\square$

Proposition 1.3.3. *Suppose $\tilde{s} \in S$, $\tilde{s} | t^e$ and $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}_S^e$. Then there is a natural isomorphism of the group $\mathrm{Ext}_{\mathrm{MF}_S^e}(\mathcal{M}_{\tilde{s}}, \mathcal{N})$ onto $Z_{\tilde{s}}(\mathcal{N})/B_{\tilde{s}}(\mathcal{N})$, where $Z_{\tilde{s}}(\mathcal{N}) = \{n \in N^0 \mid t^e \tilde{s}^{-1} n \in N^1\}$ and $B_{\tilde{s}}(\mathcal{N}) = \{v^1 - \tilde{s}\varphi_1(v^1) \mid v^1 \in N^1\}$.*

Proof. By definition, $\mathcal{M}_{\tilde{s}} = (Sm, Sm^1, \varphi_1)$, where $\varphi_1(m^1) = m$ and $m^1 = \tilde{s}m$. Suppose $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{Ext}_{\mathrm{MF}_S^e}(\mathcal{M}_{\tilde{s}}, \mathcal{N})$. Then $\mathcal{M}$ can be described as follows: $M = N^0 \oplus S\hat{m}$, $M^1 = N^1 + S\hat{m}^1$, where $\hat{m}^1 = \tilde{s}\hat{m} + n(\mathcal{M})$ with $n(\mathcal{M}) \in N^0$ and $\varphi_1(\hat{m}^1) = \hat{m}$. Notice that $M^1 \supset t^e M^0$ holds if and only if $n(\mathcal{M}) \in Z_{\tilde{s}}(\mathcal{N})$ and the morphism φ_1 is uniquely defined. Any equivalent to $\mathcal{M}$ extension $\mathcal{M}'$ can be decribed by another lifts $\hat{m}' = \hat{m} + v$, $\hat{m}'^1 = \hat{m}^1 + v^1$ with $v \in N^0$ and $v^1 \in N^1$ such that $\varphi_1(v^1) = v$. Then the corresponding element $n(\mathcal{M}')$ equals $n(\mathcal{M}) + v^1 - \tilde{s}\varphi_1(v^1)$, i.e. $n(\mathcal{M}) \equiv n(\mathcal{M}') \bmod B_{\tilde{s}}(\mathcal{N})$. Finally, a straighforward verification shows that the correspondence $\mathcal{M} \mapsto n(\mathcal{M}) \bmod B_{\tilde{s}}(\mathcal{N})$ gives the required isomorphism. $\square$

Remark 1.3.4. If $\tilde{s} \in S^*$ then we can always choose $n(\mathcal{M}) \in N^1 + tN^0$ (use that $\varphi_1(N^1)$ generates N^0).

Let $S' = S[t']$ where $t'^p = t$. Consider the extension of scalars $\mathcal{M} \mapsto \mathcal{M} \otimes_S S' \in \mathrm{MF}_{S'}^{ep}$, where $\mathcal{M} \in \mathrm{MF}_S^e$. Consider the induced group homomorphism $\pi_{SS'} : \mathrm{Ext}_{\mathrm{MF}_S^e}(\mathcal{M}_{\tilde{s}}, \mathcal{N}) \longrightarrow \mathrm{Ext}_{\mathrm{MF}_{S'}^{ep}}(\mathcal{M}_{\tilde{s}} \otimes_S S', \mathcal{N} \otimes_S S')$.

Choose a basis $n_1^1, \ldots, n_u^1$ of N^1 such that for $1 \leqslant i \leqslant u$, there are $\tilde{s}_i \in S$ such that the elements $\tilde{s}_i^{-1} n_i^1 = n_i$ form a basis of N^0. With this notation

$$Z_{\tilde{s}}(\mathcal{N}) = \left\{ \sum_i \alpha_i n_i \mid \text{ all } \alpha_i \in S \text{ and } t^e \tilde{s}^{-1} \alpha_i \equiv 0 \bmod \tilde{s}_i \right\}.$$

The module $Z_{\tilde{s}}(\mathcal{N} \otimes_S S')$ is given similarly with the only difference that all coefficients α_i should belong to S'.

Proposition 1.3.5. *With the above notation suppose $z = \sum_i \alpha_i n_i \in Z_{\tilde{s}}(\mathcal{N} \otimes_S S')$. Then $z \bmod B_{\tilde{s}}(\mathcal{N} \otimes_S S')$ belongs to the image of $\pi_{SS'}$ if and only if for all i, $\alpha_i \in S \bmod \tilde{s}_i$.*

Proof. Suppose $z \bmod B_{\tilde{s}}(\mathcal{N} \otimes_S S') = \pi_{SS'}(y)$, where $y = \sum_i \beta_i n_i \bmod B_{\tilde{s}}(\mathcal{N})$ with all $\beta_i \in S$. This means that $\sum_i \alpha_i n_i = \sum_i \beta_i n_i + v^1 - \tilde{s}\varphi_1(v^1)$, where $v^1 = \sum_i \gamma_i n_i^1 = \sum_i \gamma_i \tilde{s}_i n_i \in N^1 \otimes_S S'$. Then $\varphi_1(v^1) = \sum_i \gamma_i^p \varphi_1(n_i^1) = \sum_i \delta_i n_i \in N^0 \subset N^0 \otimes_S S'$, all $\alpha_i = \beta_i + \gamma_i \tilde{s}_i - \tilde{s}\delta_i$ and $\alpha_i \in (\beta_i - \tilde{s}\delta_i) \bmod \tilde{s}_i \in S \bmod \tilde{s}_i$.

Conversely, suppose for all i, $\alpha_i = \alpha_i^0 + \tilde{s}_i \alpha_i'$, where $\alpha_i^0 \in S$ and $\alpha_i' \in S'$. Then $\sum_i \tilde{s}_i \alpha_i' n_i \in N^1 \otimes_S S'$,

$$\sum_i \alpha_i n_i \equiv \sum_i \alpha_i^0 n_i + \tilde{s}\varphi_1 \left(\sum_i \tilde{s}_i \alpha_i' n_i \right) \bmod B_{\tilde{s}}(N \otimes_S S')$$

and the right-hand side is defined over S.The proposition is proved. $\square$

1.4. *Special bases.*

Let $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$.

Definition. An S-basis $m_1^1, \dots, m_u^1$ of M^1 will be called *special* if the non-zero images of m_i^1, $1 \leqslant i \leqslant u$, in $M^0 \bmod tM^0$ are linearly independent over k.

Suppose $m_1^1, \dots, m_u^1$ is a special basis of M^1, $m_i = \varphi_1(m_i^1)$ if $1 \leqslant i \leqslant u$, and $U \in M_u(S_1)$ is such that $(m_1^1, \dots, m_u^1) = (m_1, \dots, m_u)U$. Notice that the condition $M^1 \supset t^e M^0$ implies that U divides the scalar matrix $t^e E$ in $M_u(S)$ (where E is the unit matrix of order u), i.e. there is an $V \in M_u(S)$ such that $UV = t^e E$. Let $U = (u_{ij})$, $V = (v_{ij})$ where all entries $u_{ij}, v_{ij} \in S$.

Proposition 1.4.1. *With the above notation, if* $1 \leqslant i, j, r \leqslant u$, *then*

$$u_{ij} v_{jr} \equiv 0 \bmod t.$$

Proof. Because the basis $m_1^1, \dots, m_u^1$ is special we can assume that there is an index i_0, such that $m_1^1, \dots, m_{i_0}^1 \in tM^0$ and $m_{i_0+1}^1, \dots, m_u^1$ are linearly independent modulo tM^0. Consider the image of the equality $t^e m_r = \sum_j m_j^1 v_{jr}$ in $M^0 \bmod t$, where $1 \leqslant r \leqslant u$. This gives $0 = \sum_{i_0 < j \leqslant u} (m_j^1 \bmod t) v_{jr}$ and, therefore, $v_{jr} \in tS$ if $i_0 < j \leqslant u$. On the other hand, if $1 \leqslant j \leqslant i_0$ then $m_j^1 = \sum_i m_i u_{ij} \in tM^0$ and for any $1 \leqslant i \leqslant u$, $u_{ij} \in tS$. The proposition is proved. □

2. Construction of the functor $\mathcal{G}_O : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_O$.

2.1. *The category* Aug_O *and the functor* $\iota : \mathrm{Aug}_O \longrightarrow \mathcal{MF}_S$.

The objects of the category Aug_O are flat O-algebras A of finite rank over O with a given augmentation ideal I_A. The morphisms are morphisms of augmented algebras.

Definition. If $A \in \mathrm{Aug}_O$ then:

a) $I_A(p) := \{a \in I_A \mid a^p \in pA\}$;

b) I_A^{DP} is the maximal ideal of A with nilpotent divided powers or, equivalently, such that if $a_1 = a \in I_A^{DP}$ and for any $i \in \mathbb{N}$, $a_{i+1} = a_i^p/p$, then all $a_i \in I_A^{DP}$ and $\lim_{i \to \infty} a_i = 0$.

Notice that I_A / I_A^{DP} is killed by p (remind that $p > 2$) and we can use the identification κ_{SO} to provide I_A / I_A^{DP} with an S-module structure. Then the triple $\iota^{DP}(A) := (I_A / I_A^{DP}, I_A(p)/I_A^{DP}, \varphi_1)$, where φ_1 is induced by the correspondence $a \mapsto -a^p/p$ with $a \in I_A(p)$, is an object of the category $\mathcal{MF}_S$. The correspondence $A \mapsto \iota^{DP}(A)$ gives rise to the functor ι^{DP} from Aug_O to $\mathcal{MF}_S$.

Proposition 2.1.1. *Suppose* $A \in \mathrm{Aug}_O$, $u \geqslant 1$, $b_1, \dots, b_u \in I_A / I_A^{DP}$ *and elements* $b_1^1, \dots, b_u^1 \in I_A(p)/I_A^{DP}$ *are such that for* $1 \leqslant i \leqslant u$, $\varphi_1(b_i^1) = b_i$. *Suppose* $\hat{U} \in M_u(O)$ *is such that* $(b_1^1, \dots, b_u^1) = (b_1, \dots, b_u)\hat{U}$. *Then for* $1 \leqslant i \leqslant u$, *there are unique* $\hat{b}_i \in I_A$, $\hat{b}_i^1 \in I_A(p)$ *such that* $\hat{b}_i \bmod I_A^{DP} = b_i$, $\hat{b}_i^1 \bmod I_A^{DP} = b_i^1$, $(\varphi_1(\hat{b}_1^1), \dots, \varphi_1(b_u^1)) = (\hat{b}_1, \dots, \hat{b}_u)$ *and* $(\hat{b}_1^1, \dots, \hat{b}_u^1) = (\hat{b}_1, \dots, \hat{b}_u)\hat{U}$.

Proof. The proof is very similar to the proof of proposition 1.

Use the vector notation, e.g. $\bar{b} = (b_1, \dots, b_u)$, $\bar{b}^1 = (b_1^1, \dots, b_u^1)$. Choose $\bar{b}^{(0)1}$ with coordinates in $I_A(p)$ such that $\bar{b}^{(0)1} \bmod I_A^{DP} = \bar{b}^1$. Then define for $i \geqslant 1$,

$\bar{b}^{(i)}$ and $\bar{b}^{(i)1}$ via the relations $\bar{b}^{(i+1)} = \varphi_1(\bar{b}^{(i)1})$ and $\bar{b}^{(i)1} = b^{(i-1)}\hat{U}$. Consider the sequence of ideals J_i, $i \geqslant 0$, such that $J_0 = I_A^{DP}$ and $J_{i+1} = I_A(p)J_i + \varphi_1(J_i)$, where $\varphi_1(J_i)$ is the ideal generated by all elements $\varphi_1(a)$, $a \in J_i$. Notice that for all $i \geqslant 1$, $\bar{b}^{(i)1} \equiv \bar{b}^{(i-1)1} \bmod J_{i-1}$ and $\bar{b}^{(i)} \equiv \bar{b}^{(i-1)} \bmod J_{i-1}$. This proves our proposition because $\bigcap\limits_{i \geqslant 0} J_i = 0$. $\square$

2.2. *The family of augmented O-algebras $\mathcal{A}(\mathcal{M})$, $\mathcal{M} \in \mathrm{MF}_S^e$.*

Suppose $\mathcal{M} = (M^0, M^1, \varphi_1)$ and the coordinates of the vector $\bar{m}^1 = (m_1^1, \ldots, m_u^1)$ form a special basis in M^1. As earlier, the coordinates $m_1, \ldots, m_u$ of $\varphi_1(\bar{m}^1) = \bar{m}$ form an S-basis of M^0 and there is an $U \in M_u(S)$ such that $\bar{m}^1 = \bar{m}U$.

Choose $\hat{U} \in M_u(O)$ such that $\hat{U} \bmod p = \kappa_{SO}(U \bmod t^{ep})$. Introduce the augmented O-algebra A as a quotient of $O[Y_1, \ldots, Y_u]$ by the ideal

$$J_A := J_{A,K} \bigcap O[Y_1, \ldots, Y_u],$$

where $J_{A,K}$ is the ideal in $K[Y_1, \ldots, Y_u]$ generated by the coordinates $F_1, \ldots, F_u$ of the vector $\bar{F} = (\bar{Y}\hat{U})^{(p)} + p\bar{Y}$. By definition the augmentation ideal I_A of A is generated by $Y_1 \bmod J_A, \ldots, Y_u \bmod J_A$. Here and everywhere below we use the vector notation $\bar{Y} = (Y_1, \ldots, Y_u)$ and for any matrix $C = (c_{ij})$, $C^{(p)} := (c_{ij}^p)$. So, if $\hat{U} = (\hat{u}_{ij})$ then for $1 \leqslant i \leqslant u$, $F_i = (\sum_j Y_j \hat{u}_{ji})^p + pY_i$. If there is no risk of confusion we shall use just the notation $Y_1, \ldots, Y_u$ for the elements $Y_1 \bmod J_A, \ldots, Y_u \bmod J_A$ of A.

Proposition 2.2.1. *A is a flat O-algebra of rank p^u.*

Proof. First, we need the following property.

Lemma 2.2.2. a) *$\hat{U}^{(p)} = (\hat{u}_{ij}^p)$ divides the scalar matrix pE in $M_u(O)$;*

b) if $V^0 = (v_{ij}^0) \in M_u(O)$ is such that $\hat{U}^{(p)}V^0 = pE$ then for any $1 \leqslant i, r, j \leqslant u$,

$$\hat{u}_{ir}v_{rj}^0 \equiv 0 \bmod \pi.$$

Proof of lemma. Let $V = (v_{ij}) \in M_u(S)$ be such that $UV = t^eE$. Choose $\hat{v}_{ij} \in O$ such that for all $1 \leqslant i, j \leqslant u$, $\hat{v}_{ij} \bmod p = \kappa_{SO}(v_{ij} \bmod t^{ep})$. Then the equality $UV = t^eE$ implies that $\sum\limits_r \hat{u}_{ir}\hat{v}_{rj} \equiv \pi^e\delta_{ij} \bmod p$, where δ is the Kronecker symbol. Now Proposition 1.4.1 implies that all products $\hat{u}_{ir}\hat{v}_{rj} \equiv 0 \bmod \pi$ and, therefore,

$$\sum_r \hat{u}_{ir}^p \hat{v}_{rj}^p \equiv \pi^{ep}\delta_{ij} \bmod p\pi.$$

This gives the existence of $v'_{ij} \in O$ such that $v'_{ij} \equiv \hat{v}_{ij}^p \bmod \pi$ and

$$\sum_r \hat{u}_{ir}^p v'_{rj} = \pi^{ep}\delta_{ij}.$$

Therefore, we can take the matrix $V^0 = (v_{ij}^0) = (v'_{ij}p\pi^{-ep})$ to satisfy the requirement $\hat{U}^{(p)}V^0 = pE$. Clearly, the condition b) follows from Proposition 1.4.1.

The lemma is proved. $\square$

Continue the proof of proposition 2.2.1. Let $(F'_1, \ldots, F'_u) = ((\bar{Y}\hat{U})^{(p)} + p\bar{Y})\hat{U}^{(p)^{-1}}$. Let J'_A be the ideal in $O[Y_1, \ldots, Y_u]$ generated by $F'_1, \ldots, F'_u$. Clearly, $J'_A \otimes_O K = J_A \otimes_O K$. By above Lemma 2.2.2 all $F'_i \in O[Y_1, \ldots, Y_u]$ and, therefore, $J'_A \subset J_A$.

Definition. $O^{<p}[Y_1,\dots,Y_u]$ will denote the O-submodule in $O[Y_1,\dots,Y_u]$ generated by all monomials $Y^{\underline{i}} := Y_1^{i_1}\dots Y_u^{i_u}$, where $\underline{i} = (i_1,\dots,i_u)$ is a multi-index such that $0 \leqslant i_1,\dots,i_u < p$.

Lemma 2.2.3. *With the above notation*

$$O[Y_1,\dots,Y_u] = \oplus_{k_1,\dots,k_u \geqslant 0} O^{<p}[Y_1,\dots,Y_u] F_1'^{k_1}\dots F_u'^{k_u}.$$

Proof of lemma. First, prove that for all $1 \leqslant i \leqslant u$, $F_i' = Y_i^p + G_i'$, where $G_i' \bmod \pi \in k[Y_1,\dots,Y_s]$ are linear polynomials. Indeed, the non-linear terms of the polynomial $F_i' - \sum_j Y_j^p \hat{u}_{ji}^p$ have coefficients divisible by elements of the form $p\hat{u}_{j_1 i}\dots\hat{u}_{j_p i}$. By above Lemma 2.2.2, ${U^{(p)}}^{-1} = (v_{ij}^0/p)$. Therefore, the coefficients of non-linear terms of F_i' are linear combinations of $p\hat{u}_{j_1 i}\dots\hat{u}_{j_p i}v_{ij}^0/p \equiv 0 \bmod \pi$ because $\hat{u}_{j_1 i}v_{ij}^0 \equiv 0 \bmod \pi$.

Now the division algorythm in each variable $Y_1,\dots,Y_u$ gives the required decomposition modulo π. This immediately implies the required decomposition on the level of O-modules. The lemma is proved. $\square$

Lemma 2.2.3 implies that the projection $\mathrm{pr}_{\bar{0}}$ of $O[Y_1,\dots,Y_u]$ onto the $(0,\dots,0)$-component $O^{<p}[Y_1,\dots,Y_u]$ of the corresponding decomposition has the kernel J_A' and it identifies $O[Y_1,\dots,Y_u]/J_A'$ with the flat O-module $O^{<p}[Y_1,\dots,Y_u]$.

The embedding $J_A' \subset J_A$ induces an epimorphic map of O-modules

$$\alpha : O^{<p}[Y_1,\dots,Y_u] \longrightarrow A.$$

But $J_A' \otimes_O K = J_A \otimes_O K$ implies that $\mathrm{Ker}\,\alpha \otimes_O K = 0$ (because $O^{<p}[Y_1,\dots,Y_u]$ has no O-torsion). Therefore, $\mathrm{Ker}\,\alpha = 0$, $J_A = J_A'$ and the proposition is proved. $\square$

Remark. Notice that for any $1 \leqslant i \leqslant u$, one has $dF_i = p(1+H_i)dY_i$, where all H_i belong to the maximal ideal of the ring of formal power series $O[[Y_1,\dots,Y_u]]$. Therefore, dF_i, $1 \leqslant i \leqslant u$, form an $K[[Y_1,\dots,Y_u]]$-basis of $\Omega^1_{K[[Y_1,\dots,Y_u]]/K}$ and $A_K = A \otimes_O K$ is etale over K.

Definition. For a given $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ denote by $\mathcal{A}(\mathcal{M})$ the family of O-algebras obtained by the above procedure for all choices of a special basis in M^1 and the corresponding lift $\hat{U} \in M_u(O)$ of the matrix $\kappa_{SO}(U \bmod t^{ep}) \in M_u(O/pO)$.

2.3. *φ_1-nilpotent lifts θ_A^{DP}.*

Suppose $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ and $A \in \mathcal{A}(\mathcal{M})$ is given in the notation from n.2.2. Consider $\iota^{DP}(A) = (I_A/I_A^{DP}, I_A(p)/I_A^{DP}, \varphi_1) \in \mathcal{MF}_S$. Define the S-linear morphism $\theta_A^0 : M^0 \longrightarrow I_A/I_A^{DP}$ by the correspondences $m_i = \varphi_1(m_i^1) \mapsto Y_i \bmod I_A^{DP}$, $1 \leqslant i \leqslant u$. Then θ_A^0 induces $\theta_A^1 : M^1 \longrightarrow I_A(p)/I_A^{DP}$, which is also uniquely determined by the correspondences $m_i^1 \mapsto Z_i \bmod I_A^{DP}$, $1 \leqslant i \leqslant u$. So,

$$\theta_A^0(M^0) = N^0 = \left\{ \sum_i o_i Y_i \bmod I_A^{DP} \mid o_1,\dots,o_u \in O \right\},$$

$$\theta_A^1(M^1) = N^1 = \left\{ \sum_i o_i Z_i \bmod I_A^{DP} \mid o_1,\dots,o_u \in O \right\},$$

where for all $1 \leqslant i \leqslant u$,

$$Z_i = \sum_j Y_j \hat{u}_{ji}. \tag{2.3.1}$$

Clearly, $\varphi_1 : I_A(p)/I_A^{DP} \longrightarrow I_A/I_A^{DP}$ induces $\varphi_1 : N^1 \longrightarrow N^0$ and we obtain $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathcal{MF}_S$ together with the natural embedding $\mathcal{N} \longrightarrow \iota^{DP}(A)$ in the category $\mathcal{MF}_S$. On the other hand, it is not obvious that $\theta_A^{DP} := (\theta_A^0, \theta_A^1)$ gives a morphism from $\mathcal{M}$ to $\mathcal{N}$ in the category $\mathcal{MF}_S$: we must verify the compatibility of θ_A^{DP} with φ_1's in $\mathcal{M}$ and $\mathcal{N}$. As a matter of fact, we have more.

Proposition 2.3.2. *θ_A^{DP} is a φ_1-nilpotent morphism in the category $\mathcal{MF}_S$.*

Proof. Consider the map $\tilde{\iota}_A : M^0 \longrightarrow A \otimes O/pO$ given for $1 \leqslant i \leqslant u$, by the correspondences $m_i \mapsto \widetilde{Y}_i := Y_i \bmod p$. If $\widetilde{\mathcal{M}} := \tilde{\iota}_A(\mathcal{M}) = (\widetilde{M}^0, \widetilde{M}^1, \varphi_1)$, then

- $\widetilde{M}^0$ is a free $O/p = \kappa_{SO}(S/t^{ep})$-module with the basis $\widetilde{Y}_1, \ldots, \widetilde{Y}_u$;
- $\widetilde{M}^1$ is generated over O/p by $\widetilde{Z}_i := Z_i \bmod pA$, where $i = 1, \ldots, u$ and $Z_1, \ldots, Z_u$ are given by above relations (2.3.1);
- $\varphi_1 : \widetilde{M}^1 \longrightarrow \widetilde{M}$ is a unique σ-linear map such that $\widetilde{Z}_i \mapsto \widetilde{Y}_i$, $1 \leqslant i \leqslant u$.

Clearly, $\tilde{\iota}_A : \mathcal{M} \longrightarrow \tilde{\iota}_A(\mathcal{M})$ is φ_1-nilpotent (use that $p > 2$ and $\varphi_1(t^{ep}M^0) \subset \varphi_1(t^{e(p-1)}M^1) \subset t^{ep(p-1)}M^0$). So, if $h : \widetilde{M} \longrightarrow \theta_A^{DP}(\mathcal{M})$ is the natural projection and $T = \operatorname{Ker} h : \widetilde{M}^0 \longrightarrow N^0$ then it will be sufficient to prove that $\operatorname{Ker} h|_{\widetilde{M}^1} = T$, $\varphi_1(T) \subset T$ and $\varphi_1|_T$ is nilpotent.

Lemma 2.3.3. *If for $o_1, \ldots, o_u \in O$, $\sum_i o_i Y_i \in I_A(p)$ then $\sum_i o_i \widetilde{Y}_i \in \widetilde{M}^1$.*

Proof. If $\sum_i o_i Y_i \in I_A(p)$ then $\sum_i o_i^p Y_i^p \in pI_A$. Consider the generators $F_i' = Y_i^p + G_i'$, $1 \leqslant i \leqslant u$, of the ideal J_A from the proof of proposition 2.2.1. Then

$$\sum_i o_i^p G_i' \in pO[Y_1, \ldots, Y_u]. \tag{2.3.4}$$

Indeed, $\sum_i o_i^p Y_i^p \equiv -\sum_i o_i^p G_i' \bmod J_A$ and the polynomial from the right hand side is a canonical presentation of the element from the left hand side as a polynomial from $O^{<p}[Y_1, \ldots, Y_u]$.

Notice now that the linear terms of the coordinates of the vector $(G_1', \ldots, G_u')$ are equal to $p\bar{Y}(\hat{U}^{(p)})^{-1}$. Therefore, above condition (2.3.4) implies that

$$\hat{U}^{(p)^{-1}} \begin{pmatrix} o_1^p \\ \ldots \\ o_u^p \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \ldots \\ \alpha_n \end{pmatrix}$$

with all $\alpha_1, \ldots, \alpha_u \in O$.

Clearly, for $1 \leqslant i \leqslant u$, there are $\alpha_i' \in O$ such that $\alpha_i'^p \equiv \alpha_i \bmod p$. Then we obtain

$$\begin{pmatrix} o_1 \\ \ldots \\ o_u \end{pmatrix} \equiv \hat{U} \begin{pmatrix} \alpha_1' \\ \ldots \\ \alpha_u' \end{pmatrix} \bmod \pi^e$$

and, therefore,

$$\sum_i o_i\widetilde{Y}_i = \widetilde{\hat{Y}}\begin{pmatrix} o_1 \\ \dots \\ o_u \end{pmatrix} \equiv \widetilde{\hat{Y}}\hat{U}\begin{pmatrix} \alpha'_1 \\ \dots \\ \alpha'_u \end{pmatrix} \equiv \widetilde{\hat{Z}}\begin{pmatrix} \alpha'_1 \\ \dots \\ \alpha'_u \end{pmatrix} \bmod \pi^e.$$

In other words, $\sum_i o_i\widetilde{Y}_i$ is an O- linear combination of $\widetilde{Z}_1, \dots, \widetilde{Z}_u$ modulo $\pi^e\widetilde{M}^0$ and it remains to notice that $\pi^e\widetilde{M}^0 \subset \widetilde{M}^1$.

The lemma is proved. $\square$

- Prove that $T = \operatorname{Ker} h|_{\widetilde{M}^1}$.

Suppose $o_1, \dots, o_u \in O$ are such that $\sum_i o_i\widetilde{Y}_i \in \operatorname{Ker} h$. Then $\sum_i o_iY_i \in I_A^{DP}$. In particular, $\sum_i o_iY_i \in I_A(p)$ and $\sum_i o_i\widetilde{Y}_i \in \widetilde{M}^1$ by the above lemma. So, $T \subset \widetilde{M}^1$ and, therefore, $T = \operatorname{Ker} h|_{\widetilde{M}^1}$.

- Prove that $\varphi_1(T) \subset T$.

Let J^* be the ideal in A generated by p and all products $Z_{i_1} \dots Z_{i_p}$, where $1 \leqslant i_1, \dots, i_p \leqslant u$. Because $p > 2$ and all $Z_i \in I_A(p)$, it holds $J^* \subset I_A^{DP}$.

Suppose $o_1, \dots, o_u \in O$ and $\tilde{m} = \sum_i o_i\widetilde{Z}_i \in T$. Then $\sum_i o_iZ_i \in I_A^{DP}$ and $\varphi_1(\tilde{m})$ is the image in I_A/pI_A of $\sum_i o_i^pY_i = -p^{-1}\left(\sum_i o_iZ_i\right)^p + j^*$, where $j^* \in J^*$ (use that $Z_i^p + pY_i = 0$). This element belongs to I_A^{DP} and, therefore, $\varphi_1(\tilde{m}) \in I_A^{DP} \bmod pI_A$, i.e. $\varphi_1(\tilde{m}) \in T$.

It remains to prove that $\varphi_1|_T$ is nilpotent.

First, introduce the O-subalgebra A' of A generated by $Z_1, \dots, Z_u$. It can be described as the quotient of the polynomial ring $O[Z_1, \dots, Z_u]$ by the ideal generated by all

$$Z_i^p + pY_i = Z_i^p + p\pi^{-e}\sum_j Z_j\tilde{v}_{ji}, \quad 1 \leqslant i \leqslant u,$$

where $\tilde{V} = (\tilde{v}_{ij}) \in M_u(O)$ is such that $\hat{U}\tilde{V} = \pi^eE$. (The existence of $\tilde{V}$ follows from the existence of $V \in M_u(S)$ such that $UV = t^eE$.) This implies that any element b of A' can be written uniquely as $b = \sum_{\underline{i}} o_{\underline{i}}Z^{\underline{i}} \in O^{<p}[Z_1, \dots, Z_u]$ (as earlier, here $\underline{i} = (i_1, \dots, i_u)$, $0 \leqslant i_1, \dots, i_u < p$, all $o_{\underline{i}} \in O$ and $Z^{\underline{i}} = Z_1^{i_1} \dots Z_u^{i_u}$).

Let $I_{A'} = (Z_1, \dots, Z_u)$ be the augmentation ideal of A'.

Lemma 2.3.5. *If $\alpha_1, \dots, \alpha_u \in O$ and $\alpha_1Z_1 + \dots + \alpha_uZ_u \in I_{A'}^p + pA'$ then all $\alpha_i \in p\pi^{-e}O$.*

Proof. We have $\alpha_1Z_1 + \dots + \alpha_uZ_u + pb = a \in I_{A'}^p$, where we can assume that $b = \sum_{\underline{i}} o_{\underline{i}}Z^{\underline{i}} \in O^{<p}[Z_1, \dots, Z_u]$.

Notice that a is an O-linear combination of the terms $Z_1^{j_1} \dots Z_u^{j_u}$ with $j_1 + \dots + j_u \geqslant p$. If all $j_i < p$ then such a term can contribute only to the coefficient $o_{\underline{i}}$ from the above decomposition of b with $\underline{i} = (j_1, \dots, j_u)$ and does not affect $\alpha_1, \dots, \alpha_u$. If for some index i, $j_i \geqslant p$ then Z_i^p must be replaced by $-p\pi^{-e}\sum_j Z_j\tilde{v}_{ji}$ and a possible contribution to $\alpha_1, \dots, \alpha_u$ is zero modulo $p\pi^{-e}$.

The lemma is proved. $\square$

- Prove that $\varphi_1|T$ is nilpotent.

Suppose $m_0 \in T$. For all $i \geqslant 0$, set $m_{i+1} = \varphi_1(m_i)$.

Choose $\hat{m}_0 = \sum_k o_{k0} Z_k$ such that $\hat{m}_0 \bmod pI_A = m_0$.

Then $\hat{m}_0 \in I_A^{DP}$ and, therefore, if $u_0 = \hat{m}_0$ and for $i \geqslant 0$, $u_{i+1} = -u_i^p/p$, then $\lim\limits_{i\to\infty} u_i = 0$. Notice that all u_i belong to the augmentation ideal $I_{A'}$ of the above defined O-algebra $A' = O[Z_1, \ldots, Z_u]$.

For $i > 0$, define $\hat{m}_i = \sum_k o_{ki} Z_k$ with $o_{ki} \in O$, by the relation

$$\hat{m}_i = \sum_k o_{k,i-1}^p Y_k = \sum_k o_{ki} Z_k.$$

Clearly, $m_i = \hat{m}_i \bmod pI_A$ and there are $j_i \in I_{A'}^p$ such that

$$\hat{m}_{i+1} = -\frac{\hat{m}_i^p}{p} + j_i.$$

This means that for any $i \geqslant 0$, $\hat{m}_i \equiv u_i \bmod I_{A'}^p$. Therefore, there is an $i_1 \geqslant 0$ such that for any $i \geqslant i_1$, $\hat{m}_i \in I_{A'}^p + pI_{A'}$. Now Lemma 2.3.5 implies that $m_{i_1} \in \pi^{e(p-1)}\widetilde{M}^1$ and $\varphi_1|T$ is nilpotent because $\varphi_1(\pi^e \widetilde{M}^1) \subset \pi^{ep}\widetilde{M} \subset \pi^{e(p-1)}\widetilde{M}^1$ and $p > 2$.

The proposition is proved. $\square$

2.4. *The functor* $\mathcal{G}_O : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_O$.

Consider $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$, $A \in \mathcal{A}(\mathcal{M})$ and $B \in \mathrm{Aug}_O$.

Lemma 2.4.1. *The correspondence* $f \mapsto \theta_A^{DP} \circ \iota^{DP}(f)$ *induces a bijective map from* $\mathrm{Hom}_{\mathrm{Aug}_O}(A, B)$ *to* $\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \iota^{DP}(B))$.

Proof. Suppose $A = O[Y_1, \ldots, Y_u]$ is given in notation of n.2.2. Then by considering the images $\bar{c}$ of the vector $\bar{Y} = (Y_1, \ldots, Y_u)$ in $(I_B)^u$ we obtain

$$\mathrm{Hom}_{\mathrm{Aug}_O}(A, B) = \{\bar{c} \in (I_B)^u, \bar{c}' \in I_B(p)^u \mid -\bar{c}'^{(p)}/p = \bar{c},\ \bar{c}' = \bar{c}\hat{U}\ \}.$$

Similarly,

$$\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \iota^{DP}(B)) = \{\bar{b} \in (I_B/I_B^{DP})^u, \bar{b}' \in (I_B(p)/I_B^{DP})^u \mid \varphi_1(\bar{b}') = \bar{b}, \bar{b}' = \bar{b}\hat{U}\}.$$

The correspondence $f \mapsto \theta_A^{DP} \circ \iota^{DP}(f)$ is given by the projections $\bar{c} \mapsto \bar{c} \bmod I_B^{DP}$ and $\bar{c}' \mapsto \bar{c}' \bmod I_B^{DP}$. Therefore, our lemma follows from proposition 2.1.1. $\square$

Proposition 2.4.2. *Suppose* $\mathcal{M}_1, \mathcal{M}_2 \in \mathrm{MF}_S^e$, $A_1 \in \mathcal{A}(\mathcal{M}_1)$ *and* $A_2 \in \mathcal{A}(\mathcal{M}_2)$. *Then*

a) *for any* $g \in \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_1, \mathcal{M}_2)$, *there is a unique* $f \in \mathrm{Hom}_{\mathrm{Aug}_O}(A_1, A_2)$ *such that* $\theta_{A_1}^{DP} \circ \iota^{DP}(f) = g \circ \theta_{A_2}^{DP}$;

b) *with the above notation, the correspondence* $g \mapsto f$ *gives an embedding*

$$p_{A_1 A_2} : \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_1, \mathcal{M}_2) \longrightarrow \mathrm{Hom}_{\mathrm{Aug}_O}(A_1, A_2).$$

Proof. a) follows from Lemma 2.4.1 applied to $g \circ \theta_{A_2}^{DP} \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}_1, \iota^{DP}(A_2))$. In order to prove b) notice that $\iota^{DP}(f)(\theta_{A_1}^{DP}(\mathcal{M}_1)) = (g \circ \theta_{A_2}^{DP})(\mathcal{M}_1) \subset \theta_{A_2}^{DP}(\mathcal{M}_2)$. Therefore, g appears as a unique φ_1-nilpotent lift of

$$\theta_{A_1}^{DP} \circ \iota^{DP}(f) \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}_1, \theta_{A_2}^{DP}(\mathcal{M}_2)).$$

□

Let $\mathcal{M} \in \mathrm{MF}_S^e$ and $A \in \mathcal{A}(\mathcal{M})$. Notice that $A \otimes_O A \in \mathcal{A}(\mathcal{M} \oplus \mathcal{M})$. Indeed, suppose A is constructed via the special basis $m_1^1, \dots, m_u^1$ of M^1 and the corresponding matrix $\hat{U} \in M_u(O)$. Then $A \otimes_O A$ will appear in $\mathcal{A}(\mathcal{M} \oplus \mathcal{M})$ via the special basis $(m_1^1, 0), \dots, (m_u^1, 0), (0, m_1^1), \dots, (0, m_u^1)$ of $M^1 \oplus M^1$ and the corresponding matrix $\begin{pmatrix} \hat{U} & 0 \\ 0 & \hat{U} \end{pmatrix}$.

Then proposition 2.4.2 immediately implies that $\operatorname{Spec} A$ can be provided with a structure of the object of the category Gr_O by taking:

- $p_{A,A\otimes A}(\nabla) : A \longrightarrow A \otimes A$ as a comultiplication, where ∇ is the diagonal embedding of $\mathcal{M}$ into $\mathcal{M} \oplus \mathcal{M}$;
- the natural projection $A \longrightarrow A/I_A = O$ as a counit; notice that this projection also appears in the form p_{AO}, where O is considered as an element of $\mathcal{A}(0)$ and $0 = (0, 0, \varphi_1)$ is the zero object in MF_S^e;
- $p_{AA}(-\operatorname{id}_{\mathcal{M}})$ as a coinversion.

Now we can introduce the *functor* $\mathcal{G}_O$. For any $\mathcal{M} \in \mathrm{MF}_S^e$ choose $A = A(\mathcal{M}) \in \mathcal{A}(\mathcal{M})$ and set $\mathcal{G}_O(\mathcal{M}) = \operatorname{Spec} A(\mathcal{M})$ with the above defined structure of the object of the category Gr_O. If $\mathcal{M}_1, \mathcal{M}_2 \in \mathrm{MF}_S^e$ and $f \in \operatorname{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_1, \mathcal{M}_2)$ then set $\mathcal{G}_O(f) = p_{A(\mathcal{M}_1)A(\mathcal{M}_2)}(f)$.

We can also use proposition 2.4.2 to prove that under any other choice of representatives $A'(\mathcal{M}) \in \mathcal{A}(\mathcal{M})$, the corresponding functor $\mathcal{G}'_O$ will be naturally equivalent to $\mathcal{G}_O$.

3. Full faithfulness of $\mathcal{G}_O$.

3.1. *Special case of $B \in \mathcal{A}(\mathcal{N})$, $\mathcal{N} \in \mathrm{MF}_S^e$.*

Let $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}_S^e$. Choose an S-basis $n_1^1, \dots, n_u^1$ of N^1 such that for $1 \leqslant i \leqslant u$, there are $\tilde{s}_i \in S$ such that $n_i = n_i^1 \tilde{s}_i^{-1}$ form a basis of N^0. All $\tilde{s}_i$ divide t^e because $N^1 \supset t^e N^0$. Notice that $n_1^1, \dots, n_u^1$ is a special basis, cf. n.1.4. Indeed, for any $1 \leqslant i \leqslant u$, $n_i^1 \in tN^0$ iff $\tilde{s}_i \equiv 0 \bmod t$. Therefore, the non-zero elements of the set $\{n_i^1 \bmod tN^0 \mid \tilde{s}_i \in S^*\}$ are linearly independent over k because the corresponding elements $\tilde{s}_i^{-1} n_i$ form a part of the S-basis $n_1, \dots, n_u$ of N^0.

For $1 \leqslant i \leqslant u$, let $n'_i = \varphi_1(n_i^1)$ and let $U \in M_u(S)$ be such that $\bar{n}^1 = \bar{n}'U$. Here $\bar{n}^1 = (n_1^1, \dots, n_u^1)$ and $\bar{n}' = (n'_1, \dots, n'_u)$. Notice that $U = U_0 U_1$, where $U_0 \in \mathrm{GL}_u(S)$ is such that $\bar{n}' U_0 = \bar{n} := (n_1, \dots, n_u)$ and $U_1 = (\tilde{s}_i \delta_{ij}) \in M_u(S)$ is diagonal. Let $D \in \mathrm{GL}_u(O)$ be such that $D \bmod p = \kappa_{SO}(U_0 \bmod t^{ep})$ and let for $1 \leqslant i \leqslant u$, $\tilde{\eta}'_i \in O$ be such that $\kappa_{SO}(\tilde{s}_i \bmod t^{ep}) = \tilde{\eta}'_i \bmod p$.

Denote by $\widetilde{\Omega}$ the diagonal matrix $(\tilde{\eta}'_i \delta_{ij})$. By the results of section 2 the coordinates of the vector

$$((\bar{Y} D\widetilde{\Omega})^{(p)} + p\bar{Y})(D\widetilde{\Omega})^{(p)^{-1}} \tag{3.1.1}$$

give the equations of the algebra $B = O[\bar{Y}] \in \mathcal{A}(\mathcal{N})$. (This B corresponds to the above choice of basis $\bar{n}^1$ and the structural matrix $\hat{U} = D\widetilde{\Omega} \in M_u(O)$.)

Introduce the new variables $\bar{X} = \bar{Y} D$ and notice that $(D\widetilde{\Omega})^{(p)} = D^{(p)} \widetilde{\Omega}^{(p)}$. For $1 \leqslant i \leqslant u$, let $\eta_i = -p/\tilde{\eta}_i'^p$. With this notation, the vector (3.1.1) can be rewritten as $(\dots, X_i^p - \eta_i Y_i, \dots) D^{(p)^{-1}}$. Therefore, the algebra B appears as the quotient of

$O[X_1, \dots, X_s]$ by the ideal generated by the elements $X_i^p - \eta_i \sum_j X_j c_{ji}$, where $1 \leqslant i \leqslant s$ and $C = (c_{ij}) = D^{-1} \in \mathrm{GL}_s(O)$.

3.2 *The description of comultiplication.*

As we have just obtained, if $H = \mathcal{G}_O(\mathcal{N})$ with $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}^e$, then $A(H) = B = O[X_1, \dots, X_u]$, with the equations

$$X_i^p - \eta_i \sum_r X_r c_{ri} = 0, \quad 1 \leqslant i \leqslant u,$$

where $u = \mathrm{rk}_S N^0 = \mathrm{rk}_S N^1$, $C = (c_{ri}) \in \mathrm{GL}_u(O)$ and all $\eta_i \in O$, $\eta_i | p$.

Remark 3.2.1. We can assume that all η_i' are just integral powers of π. Indeed, the elements $\tilde{s}_i \in S$ from n.3.1 can be chosen as integral powers of t and this will allow us to choose all $\tilde{\eta}_i'$ as integral powers of π. We shall also use the notation $\tilde{\eta}_i = \tilde{\eta}_i'^p$, i.e. $\tilde{\eta}_i \eta_i = -p$.

By the definition from n.2.4, the comultiplication $\Delta : B \longrightarrow B \otimes_O B$ can be recovered uniquely from the conditions $\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i + j_i$, where all $j_i \in I^{DP}_{B \otimes B}$. Using the above equations of B we obtain the following recursive relation to recover these elements j_i:

$$\sum_r j_r c_{ri} = \tilde{\eta}_i (\phi(X_i) + \phi(X_i \otimes 1 + 1 \otimes X_i, j_i)) + j_i^p / \eta_i, \quad 1 \leqslant i \leqslant u. \tag{3.2.2}$$

Here $\phi(X, Y) = p^{-1}(X^p + Y^p - (X + Y)^p)$ is the first Witt polynomial and for all $1 \leqslant i \leqslant u$, $\phi(X_i \otimes 1, 1 \otimes X_i)$ is denoted just by $\phi(X_i)$, cf. the basic notation in the end of the Introduction.

Let $\mathcal{J}_B$ be the ideal in $B \otimes_O B$ generated by the elements $\tilde{\eta}_i X_i^r \otimes X_i^{p-r}$, where $1 \leqslant i \leqslant u$ and $1 \leqslant r < p$. Notice that all $\eta_i \phi(X_i) \in \mathcal{J}_B$. The definition of the ideal $\mathcal{J}_B$ depends on the chosen construction of the O-algebra B. But because $\tilde{\eta}_i' X_i \in I_B(p)$, all $\tilde{\eta}_i X_i^r \otimes X_i^{p-r} \in I_{B \otimes B}(p)^p$. This will allow us (if necessary) to replace $\mathcal{J}_B$ by the bigger invariant ideal $I_{B \otimes B}(p)^p$.

Proposition 3.2.3. *For all* $1 \leqslant i \leqslant u$, $j_i \in \mathcal{J}_B$.

Proof. As we above have noticed, for all i, $\tilde{\eta}_i \phi(X_i) \in \mathcal{J}_B \subset I^{DP}_{B \otimes B}$.

Consider the sequence J_n, $n \geqslant 0$, of ideals in $B \otimes B$ such that $J_0 = I^{DP}_{B \otimes B}$ and for all $n \geqslant 0$, $J_{n+1} = I_{B \otimes B}(p) J_n + \varphi_1(J_n)$, where the ideal $\varphi_1(J_n)$ is generated by the elements $\{j^p/p \mid j \in J_n\}$. Then the recursive relation (3.2.2) implies that for all $n \geqslant 0$ and $1 \leqslant i \leqslant u$, $j_i \in \mathcal{J}_B + J_n$. The proposition follows then from the fact that the intersection of all J_n is the zero ideal. □

3.3. *The ideals* $I_B(\alpha)$, $\alpha \in O$.

Notice that by Lemma 2.2.3 any element of B can be uniquely written as a linear combination $\sum_{\underline{i}} o_{\underline{i}} X^{\underline{i}} \in O^{<p}[X_1, \dots, X_u]$, where as earlier, $\underline{i} = (i_1, \dots, i_u)$, $0 \leqslant i_1, \dots, i_u < p$, $X^{\underline{i}} = X_1^{i_1} \dots X_u^{i_u}$ and all coefficients $o_{\underline{i}}$ belong to O.

Our system of generators $X_1, \dots, X_u$ has a very special property: if for all i, $X_i' = X_i^p / \eta_i$ then $X_1', \dots, X_u'$ is obtained from $X_1, \dots, X_u$ by a non-degenerate linear transformation (given by the matrix $C \in \mathrm{GL}_u(O)$). Then any element of A can

be written uniquely as a (similar to just described) linear combination $\sum_{\underline{i}} o_{\underline{i}} X'^{\underline{i}} \in O^{<p}[X'_1, \dots, X'_n]$, where $X'^{\underline{i}} = X'^{i_1}_1 \dots X'^{i_u}_{i_u}$. This follows from the fact that B is the quotient of $O[X'_1, \dots, X'_u]$ by the ideal generated by the elements

$$X'^p_i - \sum_j \eta_j X'_j c^p_{ji} + pH_i,$$

where $1 \leqslant i \leqslant u$ and all H_i are polynomials in $X'_1, \dots, X'_u$ of total degree $\leqslant p$.

Definition. For $\alpha \in O$, set

$$I_B(\alpha) = \left\{ \sum_{\underline{i}} o_{\underline{i}} X^{\underline{i}} \in O^{<p}[X_1, \dots, X_u] \mid o_{\underline{i}} \in O,\ o^p_{\underline{i}} X^{\underline{i}p} \in \alpha I_B \right\}.$$

Notice that, $\sum_{\underline{i}} o_{\underline{i}} X^{\underline{i}} \in I_B(\alpha)$ if and only if for all multi-indices $\underline{i} = (i_1, \dots, i_u)$ (where always $0 \leqslant i_1, \dots, i_u < p$), it holds $o_{\underline{i}} \in O$, $o^p_{\underline{i}} \in \alpha \eta_1^{-i_1} \dots \eta_u^{-i_u} O$ and $o_{(0,\dots,0)} = 0$.

The sets $I_B(\alpha)$ depend generally on the choice of generators $X_1, \dots, X_u$, cf. n.3.1. But if $\alpha | p$ then $I_B(\alpha) = \{a \in I_B \mid a^p \in \alpha I_B\}$ does not depend on such a choice. Notice that we have used already in 2.1 a special case of the notation $I_B(\alpha)$ when $\alpha = p$.

Lemma 3.3.1. *Suppose $o \in O$, $\alpha \in O$ and $oX^{\underline{i}} \in I_B(\alpha)$, where $\underline{i} = (i_1, \dots, i_u)$ with $0 \leqslant i_1, \dots, i_u < p$. Then for any $1 \leqslant j \leqslant u$, $oX^{\underline{i}} X_j \in I_B(\alpha \eta_j)$.*

Proof. We can assume that $j = 1$. Notice that the statement is obviously true if $i_1 < p - 1$. So, assume $i_1 = p - 1$.

Use induction on the number r of elements of the set $\{j \mid i_j \neq 0\}$.

Let $r = 1$. Then $oX^{\underline{i}} = oX_1^{p-1} \in I_B(\alpha)$ implies that $o^p \eta_1^{p-1} \equiv 0 \bmod \alpha$. Then

$$oX^{\underline{i}} X_1 = oX_1^p \in o\eta_1 I_B \subset I_B(o^p \eta_1^p) \subset I_B(\alpha \eta_1).$$

Suppose $r > 1$ and the lemma is proved for all $r' < r$. Then $oX_1^{p-1} X_2^{i_2} \dots X_u^{i_u} \in I_B(\alpha)$ means $o^p \eta_1^{p-1} \eta_2^{i_2} \dots \eta_u^{i_u} \equiv 0 \bmod \alpha$. Consider the equality

$$oX_1^{p-1} X_2^{i_2} \dots X_u^{i_u} = \sum_j o\eta_1 c_{1j} X_2^{i_2} \dots X_u^{i_u} X_j, \tag{3.3.2}$$

Then for any index j, $o\eta_1 c_{1j} X_2^{i_2} \dots X_u^{i_u} \in I_B(o^p \eta_1^p \eta_2^{i_2} \dots \eta_u^{i_u}) \subset I_B(\alpha \eta_1)$, and clearly $X_j \in I_B(1)$. Therefore, by the inductive assumption each term of the sum (3.3.2) belongs to $I_B(\alpha \eta_1)$.

The lemma is proved. □

Corollary 3.3.3. a) *If $\alpha_1, \alpha_2 \in O$ then $I_B(\alpha_1) I_B(\alpha_2) \subset I_B(\alpha_1 \alpha_2)$;*
b) *$\forall \alpha \in O$, $I_B(\alpha)$ is an ideal in B.* □

3.4. *Recovering* $\mathcal{N} \in \mathrm{MF}_S^e$.

Suppose $\mathcal{N} \in \mathrm{MF}_S^e$, $H = \mathcal{G}_O(\mathcal{N})$ and $B = A(H)$ is the algebra of H given in the notation and assumptions of n.3.2. Then use for $1 \leqslant i \leqslant n$, the generators X_i of B and the generators $X_i \otimes 1$ and $1 \otimes X_i$ of $B \otimes B$ to introduce the ideals $I_B(\alpha)$ and $I_{B\otimes B}(\alpha)$, where $\alpha \in O$.

For any $a \in I_B$, let $\delta^+ a = \Delta(a) - a \otimes 1 - 1 \otimes a \in I_{B\otimes B}$. Then by Proposition 3.2.3 for $1 \leqslant i \leqslant u$, $\delta^+ X_i \in I_{B\otimes B}(p)^p \subset I_{B\otimes B}(p^p)$.

Lemma 3.4.1. *Suppose $a \in I_B$ is such that $\delta^+ a \in I_{B\otimes B}(p^p)$. Then there are $o_1, \ldots, o_u \in O$ such that $a \equiv \sum_i o_i X_i \bmod I_B(p^p)$.*

Proof. We can assume that $a = \sum_{r(\underline{i})\geqslant 2} o_{\underline{i}} X^{\underline{i}} \in O^{<p}[X_1, \ldots, X_u]$, where as earlier $\underline{i} = (i_1, \ldots, i_u)$, $0 \leqslant i_1, \ldots, i_u < p$ and $r(\underline{i}) = i_1 + \cdots + i_u$. Then

$$\Delta(X^{\underline{i}}) \equiv (X_1 \otimes 1 + 1 \otimes X_1)^{i_1} \ldots (X_u \otimes 1 + 1 \otimes X_u)^{i_u} \bmod I_{B\otimes B}(p^p).$$

It is easy to see that:

a) $\delta^+ X^{\underline{i}}$ is a linear combination of the terms $X^{\underline{j}_1} \otimes X^{\underline{j}_2}$ where $\underline{j}_1$ and $\underline{j}_2$ are multi-indices such that $r(\underline{j}_1), r(\underline{j}_2) > 0$ and $\underline{j}_1 + \underline{j}_2 = \underline{i}$; in addition, all such terms $X^{\underline{j}_1} \otimes X^{\underline{j}_2}$ appear with coefficients from $\mathbb{Z}_p^* \subset O^*$;

b) any term $X^{\underline{j}_1} \otimes X^{\underline{j}_2}$ from the above n.a) does not appear with a non-zero coefficient in the decomposition of any $\delta^+ X^{\underline{i}_1}$ with $\underline{i}_1 \neq \underline{i}$.

The above two facts a) and b) imply that for any $\alpha \in O$ such that $\alpha | p^p$, $\delta^+ a \in I_{B\otimes B}(\alpha)$ if and only if $a \in I_B(\alpha)$. In particular, if $\alpha = p^p$ we obtain the statement of our lemma. $\square$

Let $\theta_B^{DP} : \mathcal{N} \longrightarrow \iota^{DP}(B)$ be the morphism from n.2.3 and $\theta_B^{DP}(\mathcal{N}) = (N_1^0, N_1^1, \varphi_1) \in \mathcal{MF}_S$. Then the above lemma implies that

$$\widetilde{N}^0 = \{a \in I_B \mid \delta^+ a \in I_{B\otimes B}(p)^p\}/I_B(p^p)$$

is mapped onto N_1^0 by the projection $I_B/I_B(p^p) \longrightarrow I_B/I_B^{DP}$ induced by the embedding $I_B(p^p) \subset I_B^{DP}$. Therefore, we have the following statement.

Proposition 3.4.2. *If $H = \operatorname{Spec} B = \mathcal{G}_O(\mathcal{N})$ with $\mathcal{N} \in \mathrm{MF}^e$, then $\mathcal{N}$ can be uniquely recovered as a φ_1-nilpotent lift of $(N_1^0/I_B^{DP}, N_1^1/I_B^{DP}, \varphi_1)$, where $N_1^0 = \{a \in I_B \mid \delta^+(a) \in I_{B\otimes B}(p)^p\}$, $N_1^1 = I_B(p) \cap N_1^0$ and φ_1 is induced by the map $a \mapsto -a^p/p$.*$\square$

Corollary 3.4.3. *The functor $\mathcal{G}_O$ is fully faithful.* $\square$

Remark. We could not prove that the elements of N_1^0/I_B^{DP} come from $a \in I_B$ such that $\delta^+(a) \in I_{B\otimes B}^{DP}$. This is why we use more strong condition $\delta^+(a) \in I_{B\otimes B}(p)^p$. As a matter of fact, we could use either the stronger condition $\delta^+(a) \in \mathcal{J}_B$ or the weaker one $\delta^+(a) \in I_{B\otimes B}(p^p)$, but they both depend on a choice of special generators of B and, therefore, are not functorial.

3.5. *A property of comultiplication.*

Suppose $\mathcal{N} \in \mathrm{MF}^e_S$ and $H = \mathcal{G}_O(\mathcal{N})$ is given in notation of n.3.2. Then for $1 \leqslant i \leqslant u$, $\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i + j_i$ with $j_i \in I_{B\otimes B}(p^p)$, cf. n.3.2. Remind that any element of B can be uniquely written as a polynomial from $O^{<p}[X_1, \dots, X_u]$ and any element from $B \otimes_O B$ can be uniquely written as a polynomial from $O^{<p}[X_1 \otimes 1, \dots, X_u \otimes 1, 1 \otimes X_1, \dots, 1 \otimes X_u]$. We shall use the following property later in subsection 6.7.

Proposition 3.5.1. *For $1 \leqslant i, r \leqslant u$, j_i as an element of $O^{<p}[X_1 \otimes 1, \dots, 1 \otimes X_u]$ contains $\phi(X_r)$ with the coefficient $\tilde{\eta}_r d_{ri}$ modulo $p\tilde{\eta}_r$, where $(d_{ri}) = C^{-1}$.*

Proof. We can proceed with j_i taken modulo $I_{B\otimes B}(p^{2p})$ because if $\alpha \in O$ is such that $\alpha\phi(X_r) \in I_{B\otimes B}(p^{2p})$ then $\alpha^p \eta_r^p \equiv 0 \bmod p^{2p}$ and, therefore, $\alpha \equiv 0 \bmod p\tilde{\eta}_r$.

For any $1 \leqslant i \leqslant u$, $j_i \in I_{B\otimes B}(p^p)$ and, therefore, $j_i^p/p \in I_{B\otimes B}(p^{p^2-p}) \subset I_{B\otimes B}(p^{2p})$ because $p \geqslant 3$. In addition,

$$\tilde{\eta}_i \phi(X_i \otimes 1 + 1 \otimes X_i, j_i) \in I_{B\otimes B}(p^{2p-1}).$$

Therefore, relation (3.2.2) implies that for $1 \leqslant i \leqslant u$,

$$j_i \equiv \sum_r \tilde{\eta}_r \phi(X_r) d_{ri} \bmod I_{B\otimes B}(p^{2p-1}),$$

and we obtain that

$$\sum_r j_r c_{ri} - \tilde{\eta}_i \phi(X_i) \equiv -\tilde{\eta}_i (X_i \otimes 1 + 1 \otimes X_i)^{p-1} \sum_r \tilde{\eta}_r \phi(X_r) d_{ri} \bmod I_{B\otimes B}(p^{2p}).$$

Notice that for $i \neq r$, the term $(X_i \otimes 1 + 1 \otimes X_i)^{p-1}\phi(X_r)$ does not contribute to the coefficient for $\phi(X_r)$. But if $i = r$ then

$$\tilde{\eta}_r (X_r \otimes 1 + 1 \otimes X_r)^{p-1} \tilde{\eta}_r \phi(X_r) \in p\tilde{\eta}_r I_{B\otimes B},$$

because $X_r^p \in \eta_r I_B$ and $\tilde{\eta}_r \eta_r = -p$. In other words, there is no contribution to the coefficient for $\phi(X_i)$ modulo $p\tilde{\eta}_r$. The proposition is proved. $\square$

4. Construction of the functor $\mathcal{G}^O_{O_0} : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}_{O_0}$.

In this section we use the basic notation $K, O, \pi, K_0, O_0, \pi_0$. We prove that the existence of the subfield K_0 in K implies that any $G = \mathcal{G}_O(\mathcal{M}) \in \mathrm{Gr}_O$ comes from a unique $G_0 \in \mathrm{Gr}_{O_0}$ by the extension of scalars $G_0 \mapsto G = G_0 \otimes_{O_0} O$. Then the correspondence $\mathcal{M} \mapsto G_0$ will give rise to a fully faithful functor $\mathcal{G}^O_{O_0}$ from MF^e_S to Gr_{O_0}.

4.1. *Tamely ramified extension of scalars.*

Suppose K_0' is a tamely ramified extension of K_0 with the residue field $k' \supset k$. Let O_0' be the valuation ring of K_0'. Denote by e' the absolute ramification index of K_0' and set $e_0 = e'/e$. By replacing (if necessary) K_0' by a bigger tamely ramified extension we can always assume that K_0'/K_0 is Galois and there is a uniformizer $\pi_0' \in O_0'$ such that ${\pi_0'}^{e_0} = \pi_0$. Then we can introduce $K' = K(\pi')$ with ${\pi'}^p = \pi_0'$ such that $\pi = {\pi'}^{e_0}$. Set $O' = O_{K'}$ and $\Gamma = \mathrm{Gal}(K_0'/K_0) \simeq \mathrm{Gal}(K'/K)$.

Notice, first, that there is the following necessary condition for the existence of a descent of $G'_0 \in \mathrm{Gr}_{O'_0}$ to O_0 or , resp., of $G' \in \mathrm{Gr}_{O'}$ to O (it holds without the assumption that the ramification of K'_0 over K_0 is tame):

(α) for all $\tau \in \Gamma$ there is a τ-linear bialgebra automorphism f_τ of $A(G'_0)$ (or, resp., $A(G')$) such that $\forall \tau_1, \tau_2 \in \Gamma$, $f_{\tau_1\tau_2} = f_{\tau_1} f_{\tau_2}$.

If K'_0 is unramified over K_0 then the above condition (α) is also sufficient for the existence of a such descent. If K'_0 is totally ramified over K_0 of degree n and K_0 contains a primitive n-th root of unity, then the corresponding Γ-action is semi-simple and one can easily see that G'_0 admits a descent to O_0, resp., G' admits a descent to O, if and only if the condition (α) holds and $\forall \tau \in \Gamma$, f_τ induces the identity maps on special fibres.

With the relation to the category of filtered modules introduce the appropriate characteristic p object $S' = k'[[t']]$, where $t = t'^{e_0}$. Then the identification $\kappa_{S'O'} : S'/t^{ep}S' \longrightarrow O'/pO'$ is induced by the correspondence $t' \mapsto \pi'$. This identification allows us to identify the Galois group Γ with the Galois group of $\mathrm{Frac}\, S'$ over $\mathrm{Frac}\, S$. In this situation we have the obvious functor of extension of scalars $\otimes_S S' : \mathrm{MF}^e_S \longrightarrow \mathrm{MF}^{e'}_{S'}$ and, clearly, if $\mathcal{M} \in \mathrm{MF}^e_S$ then $\mathcal{G}_{O'}(\mathcal{M} \otimes_S S') = \mathcal{G}_O(\mathcal{M}) \otimes_O O'$.

4.2. The following proposition allows us to pass to tamely ramified extensions when studying the image of the functor $\mathcal{G}_O$.

Proposition 4.2.1. *$G \in \mathrm{Gr}_O$ is in the image of the functor $\mathcal{G}_O : \mathrm{MF}^e_S \longrightarrow \mathrm{Gr}_O$ if and only if $G' = G \otimes_O O'$ is in the image of the functor $\mathcal{G}_{O'} : \mathrm{MF}^{e'}_{S'} \longrightarrow \mathrm{Gr}_{O'}$.*

Proof. It will be sufficient to consider separately the cases of an unramified extension K'_0/K_0 and a totally ramified extension K'_0/K_0 of degree n where n is prime to p and K_0 contains a primitive n-th root of unity.

Clearly, if $G = \mathcal{G}_O(\mathcal{M})$, where $\mathcal{M} \in \mathrm{MF}^e_S$, then $G' = \mathcal{G}_{O'}(\mathcal{M} \otimes_S S')$.

Now assume that $G' = \mathcal{G}_{O'}(\mathcal{M}')$, $\mathcal{M}' \in \mathrm{MF}^{e'}_{S'}$. We must prove that there is an $\mathcal{M} \in \mathrm{MF}^e_S$ such that $\mathcal{M}' = \mathcal{M} \otimes_S S'$.

For $\tau \in \Gamma$, consider τ-linear bialgebra automorphisms f_τ such that $\forall \tau_1, \tau_2 \in \Gamma$, $f_{\tau_1\tau_2} = f_{\tau_1} f_{\tau_2}$ and $A(G) = \{a \in A(G') \mid \forall \tau \in \Gamma,\ f_\tau(a) = a\}$.

By Proposition 3.4.2 there are induced τ-linear automorphisms of $\theta^{DP}_{A(G')}(\mathcal{M}')$ in the category $\mathcal{MF}_{S'}$ and by Proposition 1.2.1 they give rise to τ-linear automorphisms $g_\tau \in \mathrm{Aut}_{\mathrm{MF}^{e'}_{S'}}(\mathcal{M}')$ such that for any $\tau_1, \tau_2 \in \Gamma$, $g_{\tau_1\tau_2} = g_{\tau_1} g_{\tau_2}$.

If $\mathcal{M}' = (M'^0, M'^1, \varphi_1)$, then for any $\tau \in \Gamma$, g_τ is a τ-linear automorphism of the S'-module M'^0, $g_\tau(M'^1) = M'^1$ and $\varphi_1 g_\tau|_{M'^1} = g_\tau|_{M'^1}\varphi_1$.

If K'_0/K_0 is unramified, this already implies that for $M^0 := \{m \in M'^0 \mid \forall \tau \in \Gamma, g_\tau(m) = m\}$ and $M^1 := M^0 \cap M'^1$, it holds $\mathcal{M} = (M^0, M^1, \varphi_1|_{M^1}) \in \mathrm{MF}^e_S$ and $\mathcal{M} \otimes_S S' = \mathcal{M}'$.

If K'^0/K^0 is totally ramified then the Γ-action is semi-simple and (under our assumptions) there is an S'-basis of M'^1 such that for any $\tau \in \Gamma$, $g_\tau(m'_i) = \chi_i(\tau)m'_i$, where $1 \leqslant i \leqslant u$ and $\chi_i : \Gamma \longrightarrow k^*$ are 1-dimensional characters. Then the elements of the S'-basis $\varphi_1(m'_1), \ldots, \varphi_1(m'_u)$ of M'^0 satisfy the conditions $g_\tau(\varphi_1(m'_i)) = \chi_i(\tau)^p\varphi_1(m'_i)$,
$1 \leqslant i \leqslant u$. Therefore, $A' = A(G')$ appears in the form $O'[X_1, \ldots, X_u]$, where for all $\tau \in \Gamma$, there are induced τ-linear automorphisms $h_\tau : A' \longrightarrow A'$ such that $h_\tau(X_i) = [\chi_i(\tau)]X_i$, $1 \leqslant i \leqslant u$. (Here $[\alpha] \in O'$ is the Teichmüller representative of $\alpha \in k$.)

Notice that for all $\tau \in \Gamma$, $h_\tau = f_\tau$ by the uniqueness property from Proposition 2.4.2. It remains to notice that the elements of A' are presented uniquely as polynomials from $O'^{<p}[X_1, \dots, X_u]$. Therefore, A' can be descended to the O-algebra $A(G)$ if and only if all characters χ_i are trivial. So, there is an $\mathcal{M} \in \mathrm{MF}^e_S$ such that $\mathcal{M} \otimes_S S' = \mathcal{M}'$.

The proposition is proved. $\square$

4.3. Suppose $G_0 \in \mathrm{Gr}_{O_0}$ and $G = G_0 \otimes_{O_0} O \in \mathrm{Gr}_O$.

Proposition 4.3.1. *If $H_0 \in \mathrm{Gr}_{O_0}$ is such that $H_0 \otimes_{O_0} O = G$ then $G_0 = H_0$.*

Proof. Let $V = G(\bar{K})$ be the Γ_K-module of $\bar{K}$-points of G. Then there is a canonical embedding $A(G) \subset \mathrm{Map}^{\Gamma_K}(V, \bar{K})$ given for any $a \in A(G)$, by the correspondence

$$a \mapsto \{v \mapsto a(v) \mid \forall v \in V\}.$$

The existence of $G_0 \in \mathrm{Gr}_{O_0}$ such that $G_0 \otimes_{O_0} O = G$ implies the existence of a Γ_{K_0}-module V_0 such that $V_0|_{\Gamma_K} = V$ and $A(G_0) = A(G) \cap \mathrm{Map}^{\Gamma_{K_0}}(V_0, \bar{K})$ with respect to the natural embedding

$$\mathrm{Map}^{\Gamma_{K_0}}(V_0, \bar{K}) \subset \mathrm{Map}^{\Gamma_K}(V_0|_{\Gamma_K}, \bar{K}) = \mathrm{Map}^{\Gamma_K}(V, \bar{K}).$$

Therefore, it will be sufficient to prove that if V_0' is any Γ_{K_0}-module such that $V_0'|_{\Gamma_K} = V$ and $V_0' = H_0(\bar{K})$ with $H_0 \in \mathrm{Gr}_{O_0}$, then V_0 and V_0' coincide as Γ_{K_0}-modules.

Suppose the group morphisms $\xi : \Gamma_{K_0} \longrightarrow \mathrm{Aut}_{\mathbb{F}_p} V$ and $\xi' : \Gamma_{K_0} \longrightarrow \mathrm{Aut}_{\mathbb{F}_p} V$ give the structures of Γ_{K_0}-modules V_0 and, respectively, V_0' on V. Notice that $\xi|_{\Gamma_K} = \xi'|_{\Gamma_K}$. By Fontaine's estimates [Fo] for $e^* = ep/(p-1)$ and any $v > e^* - 1$, $\xi(\Gamma^{(v)}_{K_0}) = \xi'(\Gamma^{(v)}_{K_0}) = \mathrm{id}_V$, where $\Gamma^{(v)}_{K_0}$ is the ramification subgroup of Γ_{K_0} in the upper numbering. Therefore, ξ and ξ' factor through the natural projection $\Gamma_{K_0} \longrightarrow \Gamma_{K_0}/\Gamma^{(e^*)}_{K_0}$. Notice that $\Gamma^{(e^*)}_{K_0}$ acts non-trivially on K. (More precisely, $\Gamma^{(v)}_{K_0}$ acts trivially on K if and only if $v > e^*$.) This implies that $\Gamma_K \Gamma^{(e^*)}_{K_0} = \Gamma_{K_0}$ (use that $(\Gamma_{K_0} : \Gamma_K) = p$). So, the natural embedding $\Gamma_K \subset \Gamma_{K_0}$ induces the group epimorphism $\Gamma_K \longrightarrow \Gamma_{K_0}/\Gamma^{(e^*)}_{K_0}$. Therefore, the coincidence of ξ and ξ' on Γ_K implies that $\xi = \xi'$.

The proposition is proved. $\square$

4.4. Suppose $G \in \mathrm{Gr}_O$ and $G' = G \otimes_O O' \in \mathrm{Gr}_{O'}$.

Proposition 4.4.1. *G admits a descent to O_0 if and only if G' admits a descent to O_0'.*

Proof. It will be sufficient to consider the cases where K_0'/K_0 is unramified and totally tamely ramified of degree n, where K_0 contains a primitive n-th root of unity.

Clearly, the existence of G_0 such that $G = G_0 \otimes_{O_0} O$ implies the existence of G_0' such that $G' = G_0' \otimes_{O_0'} O'$ in both cases.

Now suppose that G_0' exists. Because $G' = G \otimes_O O'$, for any $\tau \in \Gamma$, there is a τ-linear automorphism of bialgebras $f'_\tau : A(G') \longrightarrow A(G')$ such that $\forall \tau_1, \tau_2 \in \Gamma$, $f'_{\tau_1\tau_2} = f'_{\tau_1} f'_{\tau_2}$ and in the case of totally ramified K'/K, $\forall \tau \in \Gamma$, $f'_\tau \bmod \pi' = \mathrm{id}_{A(G') \otimes k'}$.

By the uniqueness property from Proposition 4.3.1 for any $\tau \in \Gamma$, $f'_\tau|_{A(G'_0)} = f_\tau$ are τ-linear automorphisms of the coalgebra $A(G'_0)$ and they satisfy the similar properties: $\forall \tau_1, \tau_2 \in \Gamma$, $f_{\tau_1\tau_2} = f_{\tau_1} f_{\tau_2}$ and in the case of totally ramified K'_0/K_0, $\forall \tau \in \Gamma$, $f_\tau \bmod \pi'_0 = \mathrm{id}_{A(G'_0)\otimes k'}$ (because the embedding $A(G'_0) \subset A(G')$ induces the identity map on reductions). Therefore, G'_0 admits a descent G_0 to O_0 and one can easily see that $G_0 \otimes_{O_0} O = G$.

The proposition is proved. $\square$

4.5. *The Lubin-Tate group law.*

For any p-adic ring R denote by $\mathrm{m}(R)$ its topological nilradical, i.e. the ideal of all $r \in R$ such that $\lim\limits_{n\to\infty} r^n = 0$. Let

$$l_{\mathrm{LT}}(X) = X + \frac{X^p}{p} + \cdots + \frac{X^{p^n}}{p^n} + \cdots \in \mathbb{Q}_p[[X]]$$

be the Lubin-Tate logarithm. If R has no p-torsion then $\mathrm{m}(R)$ can be provided with the Lubin-Tate structure of abelian group such that for any $f, g \in \mathrm{m}(R)$, $[f] + [g] = l_{\mathrm{LT}}^{-1}(l_{\mathrm{LT}}(f) + l_{\mathrm{LT}}(g))$, cf. eg. [Ha].

We need the following simple properties:

4.5.1) for any $f, g \in \mathrm{m}(R)$, $[f] + [g] = [f + g] + [\phi_1(f, g)] + \cdots + [\phi_n(f, g)] + \ldots$, where for all $n \geqslant 1$, $\phi_n(f, g) \in \mathbb{Z}_p[X, Y]$ is a homogeneous polynomial of degree p^n and, in particular, $\phi_1(X, Y) = \phi(X, Y) = (X^p + Y^p - (X + Y)^p)/p$;

4.5.2) for any $f \in \mathrm{m}(R)$, $[p](f) = [pf] + [\alpha_1 f^p] + \cdots + [\alpha_n f^{p^n}] + \ldots$, where all $\alpha_n \in \mathbb{Z}_p$ and, in particular, $\alpha_1 = 1 - p^{p-1}$ and for $n \geqslant 2$, $\alpha_n \equiv 0 \bmod (p^{p-1})$.

4.5.3) if $X \in \mathrm{m}(R)$ then $[p](X) \equiv [X^p] + [pX] \bmod p^2 R$ (remind that $p > 2$);

4.5.4) the correspondence $a \mapsto [p](a)$ induces a one-to-one additive map from pR to $p^2 R$.

4.6. From above nn.4.2-4.4 it follows that when studying the image of the functor $\mathcal{G}_O$ we can make any tamely ramified extension of scalars. In particular, we can assume that O_0 contains a primitive p-th root of unity ζ_p. When proving that $G = \mathcal{G}_O(\mathcal{M})$, where $\mathcal{M} \in \mathrm{MF}^e_S$, is obtained via an extension of scalars from $G_0 \in \mathrm{Gr}_{O_0}$, it will be convenient to verify this only on the level of augmented algebras because of the following property.

Proposition 4.6.1. *Suppose $\zeta_p \in O_0$, $\mathcal{M} \in \mathrm{MF}^e_S$, $G = \operatorname{Spec} A = \mathcal{G}_O(\mathcal{M})$ and (A, I_A) is the corresponding augmented O-algebra. If there is an $(A_0, I_{A_0}) \in \mathrm{Aug}_{O_0}$ such that $I_{A_0} \otimes_{O_0} O = I_A$ then $\operatorname{Spec} A_0$ is provided with a unique structure of $G_0 \in \mathrm{Gr}_{O_0}$ such that $G_0 \otimes_{O_0} O = G$.*

Proof. Suppose $b_1, \ldots, b_u$ is an O_0-basis of I_{A_0}. Then it can be considered also as an O-basis of I_A. Let $\Delta : A \longrightarrow A \otimes_O A$ be the comultiplication. Then for $1 \leqslant i \leqslant u$,

$$\Delta(b_i) = b_i \otimes 1 + 1 \otimes b_i + \sum_{j,r} a^{(i)}_{jr} b_j \otimes b_r,$$

where all coefficients $a^{(i)}_{jr} \in O$. This map Δ will induce a group structure on $\operatorname{Spec} A_0$ if and only if all coefficients $a^{(i)}_{jr}$ belong to O_0.

Suppose $\tau \in \Gamma = \mathrm{Gal}(K/K_0)$. Then

$$\Delta^{(\tau)} : b_i \mapsto \sum_{j,r} \tau(a_{jr}^{(i)}) b_j \otimes b_r$$

gives a conjugate group scheme $G^{(\tau)} \in \mathrm{Gr}_O$. If f_τ is a τ-linear automorphism of A given by the action of τ on O and the trivial action on A_0 with respect to the decomposition $A = A_0 \otimes_{O_0} O$ then $\Delta^{(\tau)} = f_\tau^{-1} \circ \Delta \circ (f_\tau \otimes f_\tau)$.

Suppose $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ and G is constructed via a special basis $m_1^1, \dots, m_u^1$ of the S-module M^1, cf.n.2. If $X_1, \dots, X_u$ are the variables attached to the elements $m_i = \varphi_1(m_i^1) \in M^0$, $1 \leqslant i \leqslant u$, then Δ appears as a unique O-algebra morphism $A \longrightarrow A \otimes_O A$ such that for all i, $X_i \mapsto X_i \otimes 1 + 1 \otimes X_i \bmod I_{A\otimes A}^{DP}$. Notice that for any $\tau \in \Gamma$ and $1 \leqslant i \leqslant u$, $f_\tau(X_i) \equiv X_i \bmod I_{A\otimes A}^{DP}$. (Use that for any $c \in I_{A_0}$ and $n \geqslant 1$, $(\tau(\pi^n) - \pi^n)c \in (\zeta_p - 1)\pi I_A \subset I_A^{DP}$.) Therefore, $\Delta^{(\tau)}$ appears also as a unique morphism of O-algebras $A \longrightarrow A \otimes_O A$ such that for all i, $X_i \mapsto X_i \otimes 1 + 1 \otimes X_i \bmod I_{A\otimes A}^{DP}$. So, $\Delta^{(\tau)} = \Delta$ and the proposition is proved. $\square$

Proposition 4.6.2. *Suppose $G \in \mathcal{G}_O(\mathcal{M})$, $\mathcal{M} \in \mathrm{MF}_S^e$. Then there is $G_0 \in \mathrm{Gr}_{O_0}$ such that $G_0 \otimes_{O_0} O = G$.*

Proof. By proposition 4.6.1 it will be sufficient to show that the augmented O-algebra $A = A(G)$ comes from an augmented O_0-algebra A_0 via the extension of scalars from O_0 to O.

Suppose $|G| = p$. Then by the results of n.3, $A(G) = O[X]$, where $X^p - \eta c X = 0$ with $c \in O^*$ and $\eta \in O_0$ such that $\eta | p$, cf. Remark 3.2.1. Suppose $c = [\alpha]c_1$, where $[\alpha]$ is the Teichmuller representative of $\alpha \in k$ and $c_1 \in O^*$, $c_1 \equiv 1 \bmod \pi$. Let $c_2 = c_1^{1/(p-1)} \in O^*$, $c_2 \equiv 1 \bmod \pi$. Then

$$(c_2 X)^p - \eta[\alpha](c_2 X) = 0$$

and for the augmentation ideal $I_{A_0} = (c_2 X)A_0$ of the O_0-algebra $A_0 = O_0[c_2 X]$, we have $I_{A_0} \otimes_{O_0} O = I_{A(G)}$. This proves our proposition if $|G| = p$.

Suppose $|G| > p$.

By nn.4.2-4.4, we can replace K_0 by its sufficiently large tamely ramified extension. Therefore, we can assume that:

- there is a simplest object $\mathcal{M}_{\tilde{s}} \in \mathrm{MF}_S^e$, where $\tilde{s} \in S$ is an integral power of t, $\tilde{s} | t^e$, and there is an $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}_S^e$ such that $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{Ext}_{\mathrm{MF}_S^e}(\mathcal{M}_{\tilde{s}}, \mathcal{N})$;
- if $\tilde{\eta}' \in O$ is such that $\kappa_{SO}(\tilde{s} \bmod t^{ep}) = \tilde{\eta}' \bmod p$ then $\tilde{\eta}'^p = \tilde{\eta} \in O_0$; in addition, there is a $\tilde{\lambda}' \in O$ such that $\tilde{\eta}' = \tilde{\lambda}'^{p-1}$ and $\tilde{\lambda} = \tilde{\lambda}'^p \in O_0$ (use again Remark 3.2.1).

Describe the structures of $\mathcal{M}$ and $\mathcal{N}$. There is an S-basis $m^1, n_1^1, \dots, n_u^1$ of M^1 such that $N^1 = \sum_i S n_i^1$. There is an S-basis $m, n_1, \dots, n_u$ of M^0 such that $N^0 = \sum_i S n_i$. We can assume that for $1 \leqslant i \leqslant u$, there are $\tilde{s}_i \in S$ such that $\tilde{s}_i | t^e$, $n_i^1 = \tilde{s}_i n_i$ and $m^1 = \tilde{s} m + \sum_i \alpha_i n_i$, where $\alpha_1, \dots, \alpha_u \in S$ and $t^e \tilde{s}^{-1} \alpha_i \equiv 0 \bmod \tilde{s}_i$ (or, equivalently, $t^e \tilde{s}_i^{-1} \alpha_i \equiv 0 \bmod \tilde{s}$). The structural morphism φ_1 is given via the relations $\varphi_1(m^1) = m$ and for $1 \leqslant i \leqslant u$, $\varphi_1(n_i^1) = \sum_j n_j u_{ji}$, where $(u_{ij}) \in \mathrm{GL}_u(S)$.

Describe the structure of the corresponding O-algebra $B \in \mathcal{A}(\mathcal{N})$. It equals $B = O[X_1, \dots, X_u]$, where for $1 \leqslant i \leqslant u$, $X_i^p - \eta_i \sum_j X_j c_{ji} = 0$ with $\eta_i = -p/\tilde{\eta}_i'^p \in$

O_0, $\tilde\eta'_i \bmod p = \kappa_{SO}(\tilde s_i \bmod t_1^{ep})$ and $C = (c_{ij}) \in \mathrm{GL}_u(O)$ is such that $C \bmod p = \kappa_{SO}(u_{ij} \bmod t^{ep})$.

The structure of the corresponding $A \in \mathcal{A}(\mathcal{M})$ is given by $A = B[Y]$ where

$$\tilde\eta^{-1}\left((Y\tilde\eta' + \sum_i r_i X_i)^p + pY\right) = \left(Y + \tilde\eta'^{-1}\sum_i r_i X_i\right)^p - \eta Y = 0, \tag{4.6.3}$$

with $\tilde\eta' \bmod p = \tilde s \bmod t^{ep}$, $\tilde\eta'^p \in O_0$, $\eta = -p/\tilde\eta'^p \in O_0$ and for $1 \leqslant i \leqslant u$, $r_i \in O$, $r_i \bmod p = \alpha_i \bmod t^{ep}$ and $\eta r_i^p \equiv 0 \bmod(\tilde\eta_i)$ (or, equivalently, $\eta_i r_i^p \equiv 0 \bmod \tilde\eta$). Notice that if $\tilde\eta \in O^*$ then by Remark 1.3.3 we can assume that $\sum_i \alpha_i n_i \in M^1 + tM^0$; so, in this case we can assume that $\sum_i r_i X_i \in \mathrm{m}(B)$ and, because of equation (4.6.3) this implies that $Y \in \mathrm{m}(A)$. (Remind that $\mathrm{m}(A)$ and $\mathrm{m}(B)$ are the topological nilradicals of A and B, respectively.)

Set $h = \sum_i r_i X_i$. Then $h \in I_B$ and the above congruences imply that $h^p \in \tilde\eta I_B$. By the inductive assumption there is an augmented O_0-algebra B_0 such that $I_B = I_{B_0} \otimes_{O_0} O$. Therefore, for $0 \leqslant l < p$, there are $b_l \in I_{B_0}$ such that $h = \sum_l \pi^l b_l$.

Let $Y' \in A \otimes_O K$ be such that (we use the Lubin-Tate group law)

$$[\tilde\lambda Y'] = [\tilde\lambda Y + \tilde\lambda' h] - \sum_l [\tilde\lambda' \pi^l b_l]. \tag{4.6.4}$$

- If $\tilde\lambda \notin O^*$ then (4.6.4) implies that $Y' \equiv Y \bmod \pi I_A$.
- If $\tilde\lambda \in O^*$ then $Y \in \mathrm{m}(A)$, $h \in \mathrm{m}(B)$ and $Y' \equiv Y \bmod(Y\,\mathrm{m}(A) + \pi\,\mathrm{m}(B))$.

(Cf. the definition of $\mathrm{m}(A)$ and $\mathrm{m}(B)$ in the beginning of n.4.5.) So, in both above cases $A = B[Y']$.

Find the equation for Y'.

Multiplying (4.6.3) by $\tilde\lambda^p$ we obtain that $(\tilde\lambda Y + \tilde\lambda' h)^p + p\tilde\lambda Y = 0$. Using properties of the Lubin-Tate group law from n.4.5 we can rewrite this relation as

$$[p](\tilde\lambda Y') = [p](\tilde\lambda Y + \tilde\lambda' h) - \sum_l [p](\tilde\lambda' \pi^l b_l) \equiv$$

$$[(\tilde\lambda Y + \tilde\lambda' h)^p] + [p(\tilde\lambda Y + \tilde\lambda' h)] - \sum_l [\tilde\lambda'^p \pi_0^l b_l^p] - \sum_l [p\tilde\lambda' \pi^l b_l] \equiv$$

$$- \sum_{0 \leqslant l < p} [\tilde\lambda \pi_0^l b_l^p] \bmod p^2 I_A.$$

Therefore, by replacing Y' by $Y_1 = Y' - (p/\tilde\lambda)a$ with a suitable $a \in I_A$ we still have $A = B[Y_1]$ and Y_1 will satisfy the following relation

$$[p](\tilde\lambda Y_1) = - \sum_{0 \leqslant l < p} [\tilde\lambda \pi_0^l b_l^p]. \tag{4.6.5}$$

Notice that the right hand side of (4.6.5) equals $\tilde\lambda^p b_0$, $b_0 \in I_{B^0}$ (use that $\sum_l \pi_0^l b_l^p \equiv h^p \bmod p$ and $h^p \in \tilde\eta I_B$). If $E = \exp(X + X^p/p + \dots)$ is the Artin-Hasse exponential then $E(\tilde\lambda Y_1) = 1 + \tilde\lambda Y_2$ and we still have $A = B[Y_2]$ (this is obvious if $\tilde\lambda \notin O_0^*$ and

use that $Y_1 \in \mathrm{m}(A)$, otherwise). If $E(\tilde{\lambda}^p b_0) = 1 + \tilde{\lambda}^p b_0'$ then $b_0' \in I_{B_0}$ and Y_2 is a root of the unitary polynomial

$$F = \frac{(1+\tilde{\lambda}T)^p - 1}{\tilde{\lambda}^p} - b_0' \in B_0[T].$$

This implies (use that $\mathrm{rk}_B A = p$ and $A = B[Y_2]$) that $A = B[T]/(F)$. Therefore, for the augmented algebra $A_0 = B_0[T]/(F)$ we have $I_A = I_{A_0} \otimes_{O_0} O$.

The proposition is proved. $\square$

Corollary 4.6.6. *There is a fully faithful functor* $\mathcal{G}_{O_0}^{O} : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_{O_0}$ *such that for any* $\mathcal{M} \in \mathrm{MF}_S^e$, $\mathcal{G}_{O_0}^{O}(\mathcal{M}) \otimes_{O_0} O = \mathcal{G}_O(\mathcal{M})$. $\square$

5. Group of classes of short exact sequences in Gr_O.

In this section we do not use that the ring O is obtained from the ring O_0 by joining a p-th root of some uniformizing element of O_0. This will allow us to apply in n.6 the results of this section also to the category Gr_{O_0} with O replaced by O_0.

For technical reasons we shall assume here that the residue field $k = \bar{k}$ is algebraically closed and there is $\pi^* \in O$ such that $\pi^{*p-1} = -p$. An element $\eta \in O$ will always be such that $\eta | p$ and there is an $\lambda \in O$ such that $\lambda^{p-1} = \eta$. We set $\tilde{\lambda} = \pi^*/\lambda$ and $\tilde{\eta} = \tilde{\lambda}^{p-1}$. In particular, $\eta\tilde{\eta} = -p$ and $\lambda\tilde{\lambda} = \pi^*$.

5.1. *The different and the trace.*

Suppose $B \in \mathrm{Alg}_O$, i.e. B is a flat finite O-algebra, and A is a faithfully flat finite B-algebra.

Proposition 5.1.1. *Suppose there is* $\theta \in A$ *such that* $A = B[\theta]$. *Then:*

a) *there is a unique monic polynomial* $F \in B[X]$ *such that* $A = B[X]/(F)$ *and* $\theta = X \bmod F$*;*

b) *the ideal* $(F'(\theta))$ *does not depend on a choice of* θ*;*

c) $A_K = A \otimes_O K$ *is etale over* B_K *if and only if* $F'(\theta) \in A_K^*$.

Proof. a) follows because for any maximal ideal m in B $\dim_{B/\mathrm{m}B}(A/\mathrm{m}A)$ does not depend on m.

b) Suppose $A = B[X_1]$ and $\theta_1 = X_1 \bmod F_1$, where $F_1(X) \in B[X_1]$ is monic. Let $G(X) \in B[X]$, $H(X_1) \in B[X_1]$ be such that $\theta_1 = G(\theta)$ and $\theta = H(\theta_1)$. Then $H(G(X)) \equiv X \bmod F(X)$ implies that $H'(\theta_1)G'(\theta) \equiv 1 \bmod F'(\theta)$. In addition, $F_1(G(X)) \equiv 0 \bmod F(X)$ implies that $F_1'(\theta_1)G'(\theta) \equiv 0 \bmod F'(\theta)$. Therefore, $F_1'(\theta_1) \in (F'(\theta))$ and by symmetry $F'(\theta) \in (F_1'(\theta))$.

c) A_K is etale over B_K if and only if $\Omega^1_{A_K/B_K} = \Omega^1_{A/B} \otimes_O K = 0$. It remains to notice that $\Omega^1_{A/B} = A/(F'(\theta))dX$. $\square$

Definition. With the above notation:

a) $\mathcal{D}(A/B) = (F'(\theta))$ is the *different* of A over B;

b) if A_K is etale over B_K then we set $\mathcal{D}^{-1}(A/B) = F'(\theta)^{-1}A \subset A_K$.

Remark 5.1.2. The part a) of the above definition implies that the norm $N_{A/B}(F'(\theta))$ is the discriminant of the B-algebra A.

Let $\mathrm{Tr}_{A/B} : A \longrightarrow B$ be the trace map and let $\mathrm{Tr}_{A_K/B_K} = \mathrm{Tr}_{A/B} \otimes_O K : A_K \longrightarrow B_K$. Suppose $F(X)$ splits completely in A, i.e. there are θ_α, $1 \leqslant \alpha \leqslant \deg F$ such that $F(X) = \prod_\alpha (X - \theta_\alpha)$. For $1 \leqslant \alpha \leqslant \deg F$ introduce the O-algebra morphisms $t_\alpha : A \longrightarrow A$ such that $t_\alpha(\theta) = \theta_\alpha$ and $t_\alpha|_B = \mathrm{id}$. Clearly, for any $a \in A$, $\mathrm{Tr}_{A/B}(a) = \sum_\alpha t_\alpha(a)$.

Proposition 5.1.3. *Suppose $A = B[\theta]$, A_K is etale over B_K and $F(X)$ splits completely over A. Then there is an $a \in \mathcal{D}^{-1}(A/B)$ such that $\mathrm{Tr}_{A_K/B_K}(a) = 1$.*

Proof. This follows from the case $k = n - 1$ of the following lemma.

Lemma 5.1.4. *If $X_1, \dots, X_n$ are independent variables over $\mathbb{Q}$, $0 \leqslant k \leqslant n-1$ and δ is the Kronecker symbol then*

$$\sum_{i=1}^{n} \frac{X_i^k}{\prod_{j \neq i}(X_i - X_j)} = \delta_{k,n-1}.$$

Proof. Consider the decomposition into a sum of simplest fractions in $L(X_1)$, where $L = \mathbb{Q}(X_2, \dots, X_n)$,

$$\frac{X_1^k}{\prod_{j \neq 1}(X_1 - X_j)} = \sum_{j=2}^{n} \frac{A_j}{X_1 - X_j} + \delta_{k,n-1}. \tag{5.1.5}$$

Then multiplying this identity by $\prod_{j \neq 1}(X_1 - X_j)$ and substituting for $2 \leqslant j \leqslant n$, $X_1 = X_j$ we obtain

$$A_j = \frac{X_j^k}{\prod_{s \neq 1,j}(X_j - X_s)}.$$

It remains to substitute these formulas to (5.1.5). The lemma is proved. □

Remark 5.1.6. The above lemma implies that

$$\mathcal{D}^{-1}(A/B) = \{a \in A_K \mid \mathrm{Tr}_{A_K/B_K}(a) \in B\}.$$

5.2. *Group schemes* $\mathrm{G}_{\tilde{\lambda}}$.

Suppose $G \in \mathrm{Gr}_O$ is of order p. Then by [TO, p.14, Remark] there are $\eta, \tilde{\eta} \in O$ such that $\eta\tilde{\eta} = -p$ and $G \simeq \mathrm{G}_{\tilde{\lambda}}$, where $A(\mathrm{G}_{\tilde{\lambda}}) = O[Y_{\tilde{\lambda}}]$ with $Y_{\tilde{\lambda}}^p - \eta Y_{\tilde{\lambda}} = 0$. The counit $e_{\mathrm{G}_{\tilde{\lambda}}} : A(\mathrm{G}_{\tilde{\lambda}}) \longrightarrow O$ and the comultiplication $\Delta_{\mathrm{G}_{\tilde{\lambda}}} : A(\mathrm{G}_{\tilde{\lambda}}) \longrightarrow A(\mathrm{G}_{\tilde{\lambda}}) \otimes_O A(\mathrm{G}_{\tilde{\lambda}})$ are uniquely determined by the conditions $e_{\mathrm{G}_{\tilde{\lambda}}}(Y_{\tilde{\lambda}}) = 0$ and $\Delta_{\mathrm{G}_{\tilde{\lambda}}}(Y_{\tilde{\lambda}}) = Y_{\tilde{\lambda}} \otimes 1 + 1 \otimes Y_{\tilde{\lambda}} + \tilde{\eta}\phi(Y_{\tilde{\lambda}}) \bmod p\tilde{\eta}$. Notice, if $\tilde{\eta}_1, \tilde{\lambda}_1 \in O$, $\tilde{\eta}_1 | p$ and $\tilde{\eta}_1 = \tilde{\lambda}_1^{p-1}$ then $\mathrm{G}_{\tilde{\lambda}}$ is isomorphic to $\mathrm{G}_{\tilde{\lambda}_1}$ iff $\tilde{\eta}\tilde{\eta}_1^{-1} \in O^*$ (remind that $k = \bar{k}$).

Notice that:

a) if $\eta \in O^*$ then $\mathrm{G}_{\tilde{\lambda}}$ is etale; in particular, if $\eta = 1$ then $\mathrm{G}_{\tilde{\lambda}} = \mathrm{G}_{\pi^*}$ is constant etale;

b) if $\tilde{\eta} \in O^*$ then $\mathrm{G}_{\tilde{\lambda}}$ is multiplicative. In particular, G_1 is isomorphic to the constant multiplicative group scheme μ_p of order p given by the O-algebra $A(\mu_p) = O[T]$, where $T^p = 1$, $e(T) = 1$ and $\Delta(T) = T \otimes T$. This implies the existence of a polynomial $P \in O[X]$ such that $P(X) \equiv X \bmod X^2$, $(1 + P(Y_1))^p = 1$ and $\Delta_{\mathrm{G}_1}(1 + P(Y_1)) = (1 + P(Y_1)) \otimes (1 + P(Y_1))$.

c) there is a natural morphism of group schemes $\delta_{\tilde\lambda} : \mathrm{G}_{\tilde\lambda} \longrightarrow \mathrm{G}_1$ given by the O-algebra morphism $\delta^*_{\tilde\lambda} : O[Y_1] \longrightarrow O[Y_{\tilde\lambda}]$ such that $\delta^*_{\tilde\lambda}(Y_1) = \tilde\lambda Y_{\tilde\lambda}$. If we use the above identification $G_1 \simeq \mu_p$ then the corresponding morphism $\delta_{\tilde\lambda} : \mathrm{G}_{\tilde\lambda} \longrightarrow \mu_p$ is given by the correspondence $T \mapsto 1 + P(\tilde\lambda Y_{\tilde\lambda})$ with $P \in O[X]$ from above n.b);

d) the set of all geometric points of $\mathrm{G}_{\tilde\lambda}$ equals $\mathrm{G}_{\tilde\lambda}(O) = \{g_\alpha \mid \alpha \in \mathbb{F}_p\}$, where $g_\alpha(Y_{\tilde\lambda}) = [\alpha]\lambda$ ($[\alpha]$ is the Teichmuller representative of $\alpha \in \mathbb{F}_p$). Then for any $\alpha \in \mathbb{F}_p$ and $\delta_{\tilde\lambda} : \mathrm{G}_{\tilde\lambda} \longrightarrow \mathrm{G}_1$ from above n.c), $\delta_{\tilde\lambda}(g_\alpha) = \zeta(\alpha)$, where $\zeta(\alpha) \in O$ is the p-th root of unity uniquely determined by the congruence $\zeta(\alpha) \equiv 1 + [\alpha]\pi^* \bmod \pi^*\pi$.

5.3. $\mathrm{G}_{\tilde\lambda}$-*torsors.*

Let $B \in \mathrm{Alg}_O$. Then a $\mathrm{G}_{\tilde\lambda}$-torsor over B is a finite faithfully flat B-algebra $A \in \mathrm{Alg}_O$ with the action of $\mathrm{G}_{\tilde\lambda}$ given by an O-algebra morphism $\omega : A \longrightarrow A(\mathrm{G}_{\tilde\lambda}) \otimes_O A$ such that

- $\omega \circ (\mathrm{id} \otimes \omega) = \omega \circ (\Delta_{\mathrm{G}_{\tilde\lambda}} \otimes \mathrm{id})$;
- $B = A^{\mathrm{G}_{\tilde\lambda}} = \{a \in A \mid \omega(a) = 1 \otimes a\}$;
- the correspondence $a_1 \otimes a_2 \mapsto \omega(a_1)(1 \otimes a_2)$ induces an identification of O-algebras $A \otimes_B A = A(\mathrm{G}_{\tilde\lambda}) \otimes_O A$.

Suppose A_1 is another $\mathrm{G}_{\tilde\lambda}$-torsor over B with the $\mathrm{G}_{\tilde\lambda}$-action given by $\omega_1 : A_1 \longrightarrow A(\mathrm{G}_{\tilde\lambda}) \otimes A_1$. Then A and A_1 are equivalent if there is an isomorphism of B-algebras $\nu : A \longrightarrow A_1$ such that $\nu \circ \omega_1 = \omega \circ (\mathrm{id} \otimes \nu)$.

The set $E(\mathrm{G}_{\tilde\lambda}, B)$ of equivalence classes of $\mathrm{G}_{\tilde\lambda}$-torsors over B has a natural structure of abelian group given by the Baer composition $*$. Remind that $A * A_1 = (A \otimes_B A_1)^{\mathrm{G}_{\tilde\lambda}}$ where $\mathrm{G}_{\tilde\lambda}$ acts on $A \otimes_B A_1$ via the composition of the antidiagonal embedding into $\mathrm{G}_{\tilde\lambda} \times \mathrm{G}_{\tilde\lambda}$ and the component-wise action $\omega \otimes \omega_1$ of $\mathrm{G}_{\tilde\lambda} \times \mathrm{G}_{\tilde\lambda}$ on $A \otimes_B A_1$.

5.4. *Construction of* $\mathrm{G}_{\tilde\lambda}$-*torsors.*

As earlier, $B \in \mathrm{Alg}_O$ and $\mathrm{m}(B)$ is the topological nilradical of B.

Denote by $\hat{\mathbb{G}}_{m,\tilde\lambda}$ the formal group functor such that if B is an O-algebra then $\hat{\mathbb{G}}_{m,\tilde\lambda}(B) = (1 + (\tilde\lambda B \cap \mathrm{m}(B))^\times$. If $\tilde\lambda = 1$ we shall use also the usual notation $\hat{\mathbb{G}}_m$ for $\hat{\mathbb{G}}_{m,1}$.

Suppose $1 + \tilde\lambda^p b \in \hat{\mathbb{G}}_{m,\tilde\lambda^p}(B)$. Let A be the quotient of the polynomial ring $B[X]$ by the ideal generated by the monic polynomial $F_b(X) = \tilde\lambda^{-p}((1 + \tilde\lambda X)^p - 1) - b$. Denote the image of X in A by θ_b, then $A = B[\theta_b]$ is a faithfully flat B-algebra.

For $\alpha \in \mathbb{F}_p$, there is a unique O-algebra isomorphism $t_\alpha : A \longrightarrow A$ such that $t_\alpha|_B = \mathrm{id}$ and

$$t_\alpha : 1 + \tilde\lambda\theta_b \mapsto (1 + \tilde\lambda\theta_b)\zeta(\alpha), \tag{5.4.1}$$

where $\zeta(\alpha)$ is the p-th root of unity such that $\zeta(\alpha) \equiv 1 + [\alpha]\pi^* \bmod \pi^*\pi$. Indeed, the correspondence (5.4.1) determines a unique K-algebra automorphism $t_{\alpha K} : A_K \longrightarrow A_K$, where $A_K = A \otimes_O K$, and clearly $t_\alpha(A) \subset A$ (use that $\tilde\lambda|\pi^*$).

Proposition 5.4.2. a) *There is a unique action of* $\mathrm{G}_{\tilde\lambda}$ *on* A *given by the* O*-algebra homomorphism* $\omega : A \longrightarrow A(\mathrm{G}_{\tilde\lambda}) \otimes_O A$ *such that for any* $\alpha \in \mathbb{F}_p$, $\omega \circ (g_\alpha \otimes 1) = t_\alpha$, *where* $g_\alpha \in \mathrm{G}_{\tilde\lambda}(O)$ *were defined in 5.2 d), and this action determines on* A *a structure of* $\mathrm{G}_{\tilde\lambda}$*-torsor over* B*;*

b) *the correspondence* $1+\tilde{\lambda}^p b \mapsto A = B[\theta_b]$ *determines a group epimomorphism* $\kappa : \hat{\mathbb{G}}_{m,\tilde{\lambda}^p}(B) \longrightarrow E(\mathrm{G}_{\tilde{\lambda}}, B)$ *and* $\operatorname{Ker}\kappa = \hat{\mathbb{G}}_{m,\tilde{\lambda}}(B)^p$.

Proof. Notice that for any $\alpha \in \mathbb{F}_p$, $g_\alpha(1+P(\tilde{\lambda}Y_{\tilde{\lambda}})) = \zeta(\alpha)$. Therefore, the only candidate for such action of $\mathrm{G}_{\tilde{\lambda}}$ must satisfy the following requirement

$$\omega : 1+\tilde{\lambda}\theta_b \mapsto (1+P(\tilde{\lambda}Y_{\tilde{\lambda}}))\otimes(1+\tilde{\lambda}\theta_b). \tag{5.4.3}$$

Clearly, this requirement determines a unique O-algebra homomorphism $\omega : A \longrightarrow A(\mathrm{G}_{\tilde{\lambda}})\otimes_O A$.

Let $\mathrm{G}_{\tilde{\lambda},K} = \mathrm{G}_{\tilde{\lambda}}\otimes_O K$. Prove that $\omega_K := \omega\otimes K$ defines a $\mathrm{G}_{\tilde{\lambda},K}$-torsor over $B_K = B\otimes_O K$.

Notice that $\delta_{\tilde{\lambda}}\otimes K$ determines the identification $\mathrm{G}_{\tilde{\lambda},K} = \mu_{p,K} = \mu_p\otimes K$. Then $\omega_K(1+\tilde{\lambda}\theta_b) = T\otimes(1+\tilde{\lambda}\theta_b)$, where $A(\mu_{p,K}) = K(T)$ with the comultiplication $\Delta(T) = T\otimes T$. Therefore, $\omega_K\otimes(\mathrm{id}\otimes\omega_K) = \omega_K\otimes(\Delta\otimes\mathrm{id})$, i.e. $\mathrm{G}_{\tilde{\lambda},K}$ acts on A_K. Similarly, $A_K^{\mu_{p,K}} = B_K$, and the correspondence $a_1\otimes a_2 \mapsto \omega_K(a_1)(1\otimes a_2)$ gives an isomorphism ξ_K of K-algebras $A_K\otimes_{B_K} A_K$ and $A(\mu_{p,K})\otimes_K A_K$.

Therefore, $\omega\circ(\mathrm{id}\otimes\omega) = \omega\circ(\Delta_{\mathrm{G}_{\tilde{\lambda}}}\otimes\mathrm{id})$, because $A\subset A_K$ amd ω_K maps A into $A(\mathrm{G}_{\tilde{\lambda}})\otimes A$. We have also that $A^{\mathrm{G}_{\tilde{\lambda}}} = (A_K^{\mu_{p,K}})\cap A = B_K\cap A = B$. Finally, ξ_K induces an embedding of O-algebras $\xi : A\otimes_B A \longrightarrow A(\mathrm{G}_{\tilde{\lambda}})\otimes_O A$ such that $\xi|_{1\otimes A} = \mathrm{id}$. Now notice that

$$\mathcal{D}(A\otimes_B A/1\otimes A) = \mathcal{D}(A/B) = (\eta) = \mathcal{D}(A(\mathrm{G}_{\tilde{\lambda}})/O) = \mathcal{D}(A(\mathrm{G}_{\tilde{\lambda}})\otimes_O A/1\otimes A).$$

(Use that A is a faithfully flat B- and O-algebra, $F_b'(\theta_b) = \eta(1+\tilde{\lambda}\theta_b)^{p-1}$ and $(1+\tilde{\lambda}\theta_b)^p = 1+\tilde{\lambda}^p b\in B^*$.) Therefore, the discriminants of both $(1\otimes A)$-algebras, $A\otimes_B A$ and $A(\mathrm{G}_{\tilde{\lambda}})\otimes_O A$ are equal, and the embedding ξ is an isomorphism. The part a) is proved.

One can see easily that the map κ from the part b) of our proposition is a group homomorphism and its kernel is $\hat{\mathbb{G}}_{m,\tilde{\lambda}}(B)^p$. It remains to prove that κ is epimorphic.

Suppose $A\in E(\mathrm{G}_{\tilde{\eta}}, B)$.

First, prove that we can use the concept of the differente for the B-algebra A. We need the following properties:

1) there is an $\theta\in A$ such that $A = B[\theta]$;

2) A_K is etale over B_K;

3) $\mathcal{D}(A/B) = (\eta)$ and, therefore, is an invertible ideal of A in A_K.

Indeed, we know that $B_1 = B/\mathrm{m}(B)$ is a product of finitely many copies of k. Therefore, the B_1-algebra $A_1 = A/\mathrm{m}(B)A$ can be provided with augmentation (use that k is algebraicly closed). This implies that $E(\mathrm{G}_{\tilde{\lambda}}\otimes k, B_1) = 0$ and $A_1 = A(\mathrm{G}_{\tilde{\lambda}}\otimes B_1) = A(\mathrm{G}_{\tilde{\lambda}})\otimes B_1 = B_1[Y_{\tilde{\lambda}}]$. So, by the Nakayama Lemma, $A = B[\theta]$, where $\theta\in A$ is such that $\theta \bmod \mathrm{m}(B)A = Y_{\tilde{\lambda}}$. The identification $A\otimes_B A = A(\mathrm{G}_{\tilde{\lambda}})\otimes_O A$ implies that $A_K\otimes_{B_K} A_K$ is etale $1\otimes A_K$-algebra (because $A(\mathrm{G}_{\tilde{\lambda}})\otimes K$ is etale over K) and by faithful flatness A_K is etale over B_K. Finally, $\mathcal{D}(A/B)\otimes_B A = \mathcal{D}(A(\mathrm{G}_{\tilde{\lambda}})/O)\otimes_O A = (\eta A)\otimes_B A$ implies by faithful flatness that $\mathcal{D}(A/B) = (\eta)$.

Next, prove the existence of $v\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(A)$ such that $\omega(v) = T\otimes v$, where $T = 1+P(\tilde{\lambda}Y_{\tilde{\eta}})\in A(\mathrm{G}_{\tilde{\lambda}})$, cf. 5.2.

1st case. $\tilde{\lambda} \in O^*$.

In this case $A(\mathrm{G}_{\tilde{\lambda}}) \simeq A(\mu_p) = O[T]$, $e(T) = 1$ and $\Delta(T) = T \otimes T$. We know that $A \bmod \mathrm{m}(B)A = O[T] \otimes_O B_1$, where $B_1 = B/\mathrm{m}(B)$. Let $\theta \in A$ be such that $\theta \bmod \mathrm{m}(B)A = T \otimes 1$, then $\theta \equiv 1 \bmod \mathrm{m}(A)$ and $\omega(\theta) \equiv T \otimes \theta \bmod \mathrm{m}(B)A$. Therefore, if $\omega(\theta) = \sum_{0 \leqslant i < p} T^i \otimes a_i \in A(\mu_p) \otimes A$ then $a_1 \equiv \theta \bmod \mathrm{m}(B)A$ and, therefore, $a_1 \equiv 1 \bmod \mathrm{m}(A)$. On the other hand,

$$(\omega \circ (\mathrm{id} \otimes \omega))(\theta) = \sum_i T^i \otimes \omega(a_i) = (\Delta \otimes \mathrm{id})(\omega(\theta)) = \sum_i T^i \otimes T^i \otimes a_i$$

implies that $\omega(a_1) = T \otimes a_1$ and we can take $v = a_1$.

2nd case. $\tilde{\lambda} \notin O^*$, i.e. $\tilde{\eta} = -p\eta^{-1} \notin O^*$.

By Proposition 5.1.3 we can choose $\theta \in A$ such that $\mathrm{Tr}_{A/B}\, \theta = \eta$. Clearly, $\theta \notin B$, otherwise, $\eta \equiv 0 \bmod p$ and $\tilde{\eta} \in O^*$. Then there is $1 \leqslant m < p$ such that

$$v_1 = \sum_{\alpha \in \mathbb{F}_p} \zeta(\alpha)^m t_\alpha(\theta) \neq 0.$$

Indeed, otherwise, for all $1 \leqslant m < p$, $\sum_\alpha \zeta(\alpha)^m (t_\alpha(\theta) - \theta) = 0$ and this implies that for all $\alpha \in \mathbb{F}_p$, $t_\alpha(\theta) = \theta$, i.e. $\theta \in B$.

Let $(1 + P(\tilde{\lambda} Y_{\tilde{\lambda}}))^m = 1 + \tilde{\lambda} h$, $h \in A(\mathrm{G}_{\tilde{\lambda}})$. Then for all $\alpha \in \mathbb{F}_p$,

$$g_\alpha(1 + \tilde{\lambda} h) = \zeta(\alpha)^m = e_{\mathrm{G}_{\tilde{\lambda}}}(1 + \tilde{\lambda} t_\alpha(h)).$$

(In this situation $t_\alpha : A(\mathrm{G}_{\tilde{\lambda}}) \longrightarrow A(\mathrm{G}_{\tilde{\lambda}})$ is just the shift by $g_\alpha \in \mathrm{G}_{\tilde{\lambda}}(O)$.) Then by Proposition 5.1.3

$$v_1 - \eta = \tilde{\lambda}(e_{\mathrm{G}_{\tilde{\lambda}}} \otimes \mathrm{id}) \sum_\alpha t_\alpha(h) \otimes t_\alpha(\theta) = \tilde{\lambda}(e_{\mathrm{G}_{\tilde{\lambda}}} \otimes \mathrm{id})\, \mathrm{Tr}(h \otimes \theta) \in \tilde{\lambda}\eta A,$$

where Tr is the trace map on $A(\mathrm{G}_{\tilde{\lambda}}) \otimes A$ induced by the diagonal action of $\mathrm{G}_{\tilde{\lambda}}$. So, $v_1 = \eta(1 + \tilde{\lambda} a_1)$ with $a_1 \in A$ and for any $\alpha \in \mathbb{F}_p$, $t_\alpha(1 + \tilde{\lambda} a_1) = \zeta(\alpha)^m (1 + \tilde{\lambda} a_1)$.

The required element v then can be obtained by taking m'-th power of $1 + \tilde{\lambda} a_1$, where $mm' \equiv 1 \bmod p$. The second case is also considered.

Finally, for the above constructed element v, we have $v^p = 1 + \tilde{\lambda}^p b \in \hat{\mathbb{G}}_{m, \tilde{\lambda}^p}(B)$ and the corresponding $\mathrm{G}_{\tilde{\lambda}}$-torsor $\kappa(v^p) \in E(\mathrm{G}_{\tilde{\lambda}}, B)$ is identified with a B-subalgebra A' in A. But the differentes $\mathcal{D}(A/B)$ and $\mathcal{D}(A'/B)$ are both equal to (η). Therefore, the discriminants of A and A' over B are equal and $A = A'$. The proposition is proved. $\square$

5.5. Suppose $H = \operatorname{Spec} B$ is a finite flat commutative group scheme over O with the counut e and the comultiplication Δ. Denote by $\mathrm{Ext}(H, \mathrm{G}_{\tilde{\lambda}})$ the group of equivalence classes of short exact sequences $0 \longrightarrow \mathrm{G}_{\tilde{\lambda}} \longrightarrow G \longrightarrow H \longrightarrow 0$ in the category Gr'_O of commutative finite flat group schemes over O. (Notice that we do not assume that H and G belong to Gr_O, i.e. are killed by p.)

Definition. a) $Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ is the group of all symmetric (with respect to the permutation of factors in $B\otimes B$) $\varepsilon\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_{B\otimes B})$ such that

$$(\Delta\otimes \mathrm{id}_B)(\varepsilon)\cdot(\varepsilon\otimes 1)=(\mathrm{id}_B\otimes\Delta)(\varepsilon)\cdot(1\otimes\varepsilon).$$

b) $B^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ is the multiplicative group of all elements of the form $\delta^{\times}a:=\Delta(a)(a\otimes a)^{-1}$, where $a\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_B)$.

Then $B^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ is a subgroup in $Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ and we set $H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})=Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})/B^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$.

If $\varepsilon\in Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ then $\varepsilon^p\in Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}^p})$ and the correspondence $\varepsilon\mapsto\varepsilon^p$ induces the group homomorphism $\mathcal{F}: H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})\longrightarrow H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}^p})$.

Definition. $H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})_p:=\mathrm{Ker}\,\mathcal{F}$.

Proposition 5.5.1. *There is a functorial in H group isomorphism*

$$\mathrm{Ext}(H,\mathrm{G}_{\tilde{\lambda}})=H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})_p.$$

Proof. Suppose $G\in\mathrm{Ext}(H,\mathrm{G}_{\tilde{\lambda}})$. Then $A=A(G)$ is provided with a natural action of $\mathrm{G}_{\tilde{\lambda}}\subset G$ and with respect of this action A becomes an element of the group of torsors $E(B,\mathrm{G}_{\tilde{\lambda}})$.

By Proposition 5.4.2, $A=B[\theta]$, where for $v=1+\tilde{\lambda}\theta\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_A)$, it holds $v^p=1+\tilde{\lambda}^p b_0\in\hat{\mathbb{G}}_{m,\tilde{\lambda}^p}(I_B)$ (use the existence of counit $e_G: A\longrightarrow O$). Then $\Delta_G|_B=\Delta$ and $\Delta_G(1+\tilde{\lambda}\theta)=(1+\tilde{\lambda}\theta)\otimes(1+\tilde{\lambda}\theta)\varepsilon$, where $\varepsilon\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_{B\otimes B})$ (use that Δ_G relates the actions of $\mathrm{G}_{\tilde{\lambda}}$ and $\mathrm{G}_{\tilde{\lambda}}\times\mathrm{G}_{\tilde{\lambda}}$ via the composition $\mathrm{G}_{\tilde{\lambda}}\times\mathrm{G}_{\tilde{\lambda}}\longrightarrow\mathrm{G}_{\tilde{\lambda}}$) and, in addition, $\varepsilon\in Z^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ (use the coassociativity and commutavity of Δ_G and the existence of counit e_G).

The above $v\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_A)$ is well-defined modulo the subgroup $\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_B)$, this implies that G depends only on the class $\mathrm{cl}(\varepsilon)\in H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})$ of ε. (If we change v by va with $a\in\hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_B)$, then ε will be changed by $\varepsilon\delta^{\times}a$.) Clearly, $\varepsilon^p\in B^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}^p})$ and, therefore, we have the map $\Pi:\mathrm{Ext}(H,\mathrm{G}_{\tilde{\lambda}})\longrightarrow H^2(H,\hat{\mathbb{G}}_{m,\tilde{\lambda}})_p$. Then a straightforward verification shows that Π is a group isomorphism. $\square$

Now suppose that $H\in\mathrm{Gr}_O$ and denote by $\mathrm{Ext}_{\mathrm{Gr}_O}(H,\mathrm{G}_{\tilde{\lambda}})$ the subgroup of extensions $G\in\mathrm{Ext}(H,\mathrm{G}_{\tilde{\lambda}})$ such that $G\in\mathrm{Gr}_O$. Consider the map

$$\delta_{\tilde{\lambda}*}:\mathrm{Ext}(H,\mathrm{G}_{\tilde{\lambda}})\longrightarrow\mathrm{Ext}(H,\mu_p),$$

where $\delta_{\tilde{\lambda}}:\mathrm{G}_{\tilde{\lambda}}\longrightarrow\mu_p$ is the morphism from 5.2.1 c). Let $\bar{O}$ be the valuation ring of an algebraic closure $\bar{K}$ of K. Clearly, for any $G\in\mathrm{Ext}(H,\mu_p)$,

$$G\in\mathrm{Gr}_O\quad\Leftrightarrow\quad(\delta_{\tilde{\lambda}*}G)\otimes_O\bar{O}\in\mathrm{Ext}_{\mathrm{Gr}_{\bar{O}}}(\bar{H},\bar{\mu}_p).$$

(Here $\bar{H}=H\otimes_O\bar{O}$ and $\bar{\mu}_p=\mu_p\otimes_O\bar{O}$).

Lemma 5.5.2. $\mathrm{Ext}_{\mathrm{Gr}_{\bar{O}}}(\bar{H}, \bar{\mu}_p) = 0$.

Proof. By the Cartier duality we must prove that $\mathrm{Ext}_{\mathrm{Gr}_{\bar{O}}}((\mathbb{Z}/p)_{\bar{O}}, \bar{H}^D) = 0$, where $\bar{H}^D$ is the Cartier dual for $\bar{H}$ and $(\mathbb{Z}/p)_{\bar{O}}$ is the constant group scheme of order p over $\bar{O}$. Equivalently, we must prove that in the category $\mathrm{Gr}_{\bar{O}}$ any faithfully flat morphism $\gamma : \bar{G} \longrightarrow (\mathbb{Z}/p)_{\bar{O}}$ has a section $\hat{\gamma} : (\mathbb{Z}/p)_{\bar{O}} \longrightarrow \bar{G}$.

Consider the $\bar{O}$-algebra $C = A\left((\mathbb{Z}/p)_{\bar{O}}\right) = \oplus_{i \in \mathbb{Z}/p} \bar{O}\theta_i$, where for any $i \in \mathbb{F}_p = (\mathbb{Z}/p)_{\bar{O}}(\bar{O})$, θ_i is its characteristic function. Notice that $\sum_i \theta_i = 1$. In these terms the corresponding counit e_C and the comultiplication Δ_C are defined as follows: $e_C(\theta_0) = 1$, $e_C(\theta_i) = 0$ if $i \neq 0$, and for all i, $\Delta_C(\theta_i) = \sum_{j_1+j_2=i} \theta_{j_1} \otimes \theta_{j_2}$. Fix a section $s : \mathbb{F}_p \longrightarrow \bar{G}(\bar{O})$ of the map induced by γ on geometric points of $\bar{G}$ and $(\mathbb{Z}/p)_{\bar{O}}$. (Such section exists because $\bar{G}$ is killed by p.) Prove that the section $\hat{\gamma}$ of γ can be defined by the $\bar{O}$-linear morphism $\hat{\gamma}^* : A(\bar{G}) \longrightarrow C$ such that for any $a \in A(\bar{G})$, $\hat{\gamma}^*(a) = \sum_i a(s(i))\theta_i$.

Clearly, $\hat{\gamma}^*$ is a morphism of $\bar{O}$-algebras and $\hat{\gamma}^*|_C = \mathrm{id}_C$. It remains to verify that $\hat{\gamma}^*$ is compatible with the comultiplications Δ on $A(\bar{H}^D)$ and Δ_C on C. Let $a \in A(\bar{H}^D)$. Then

$$\Delta_C(\hat{\gamma}^*(a)) = \Delta_C(\sum_i a(s(i))\theta_i) = \sum_{j_1,j_2} a(s(j_1+j_2))\theta_{j_1} \otimes \theta_{j_2}$$

$$= \sum_{j_1,j_1} \Delta(a)(s(j_1), s(j_2))\theta_{j_1} \otimes \theta_{j_2} = (\hat{\gamma}^* \otimes \hat{\gamma}^*)(\Delta(a)).$$

The lemma is proved. □

So, the elements of $\mathrm{Ext}_{\mathrm{Gr}_O}(H, \mathrm{G}_{\tilde{\lambda}})$ are described via the classes $\mathrm{cl}(\varepsilon) \in H^2(H, \hat{\mathbb{G}}_{m,\tilde{\lambda}})_p$ such that $\delta_{\tilde{\lambda}*}(\varepsilon) \otimes_O \bar{O} \in B^2(\bar{H}, \hat{\mathbb{G}}_m)$. We can state this result in the following form.

Proposition 5.5.3. *Let $H \in \mathrm{Gr}_O$, $B = A(H)$, $\bar{B} = B \otimes_O \bar{O}$. Let $\mathcal{H}$ be the subgroup of $\hat{\mathbb{G}}_m(I_{\bar{B}})$ consisting of $\bar{f} \in 1 + \mathrm{m}(I_{\bar{B}})$ such that*

α) $\bar{f}^p \in \hat{\mathbb{G}}_{m,\tilde{\lambda}^p}(I_B)$;

β) $\delta^\times \bar{f} = \Delta(\bar{f})(\bar{f} \otimes \bar{f})^{-1} \in \hat{\mathbb{G}}_{m,\tilde{\lambda}}(I_{B\otimes B})$.

Then there is a group epimorphism $\Theta : \mathcal{H} \longrightarrow \mathrm{Ext}_{\mathrm{Gr}_O}(H, \mathrm{G}_{\tilde{\lambda}})$ such that for $\bar{f} \in \mathcal{H}$, $\Theta(\bar{f}) = \mathrm{Spec}\, A \in \mathrm{Gr}_O$ with the counit e and the comultiplication Δ such that:

1) $A = B[X]$, *where* $\tilde{\lambda}^{-p}\left((1+\tilde{\lambda}X)^p - \bar{f}^p\right) = 0$;

2) $e(X) = 0$;

3) $1 + \tilde{\lambda}\Delta(X) = [(1+\tilde{\lambda}X) \otimes (1+\tilde{\lambda}X)] \cdot \delta^\times \bar{f}$. □

Consider $\mathrm{m}(I_{\bar{B}}) = I_{\bar{B}} \cap \mathrm{m}(\bar{B})$ with the Lubin-Tate addition, cf. 4.5. For any $\bar{f} \in \mathrm{m}(I_{\bar{B}})$, set

$$\delta_{\mathrm{LT}}(\bar{f}) = [\Delta(\bar{f})] - [\bar{f} \otimes 1] - [1 \otimes \bar{f}] \in \mathrm{m}(I_{\bar{B}\otimes\bar{B}}).$$

Then the above proposition can be stated in the following equivalent form.

Proposition 5.5.4. *Let $\mathcal{H}_{\mathrm{LT}} \subset \mathrm{m}(I_{\bar{B}})$ be the subgroup (with respect to the Lubin-Tate addition) of $\bar{f} \in \mathrm{m}(I_{\bar{B}})$ such that*

α_{LT}) $[p](\bar{f}) \in \tilde{\lambda}^p I_B$;

β_{LT}) $\delta_{\mathrm{LT}}(\bar{f}) \in \tilde{\lambda} I_{B\otimes B}$.

Then there is a group epimorphism $\Theta_{\mathrm{LT}} : \mathcal{H}_{\mathrm{LT}} \longrightarrow \mathrm{Ext}_{\mathrm{Gr}_O}(H, \mathrm{G}_{\tilde{\lambda}})$ such that $\forall \bar{f} \in \mathcal{H}_{\mathrm{LT}}$, $\Theta_{\mathrm{LT}}(\bar{f}) = \Theta(E(\bar{f}))$, where E is the Artin-Hasse exponential. $\square$

Notice that this proposition is obtained from proposition 5.5.3 just by applying the Lubin-Tate logarithm. As a matter of fact this is a first (though completely trivial) step towards relating the multiplicative structures in the description of extensions from $\mathrm{Ext}_{\mathrm{Gr}_O}(H, G_{\tilde{\lambda}})$ in this section with additive constructions of the algebra and coalgebra structures of group schemes from $\mathrm{Im}\,\mathcal{G}_O$ in Sections 2 and 3.

6. Calculations in the O-algebra of $H \in \mathrm{Im}\,\mathcal{G}_O$.

In this section we use earlier notation and assumptions about S, O, O_0, t, π, π_0.

6.1. *Reminder and the statement of the Main Lemma.*

Remind earlier notation and agreements:

• $\mathcal{N} \in \mathrm{MF}^e_S$, $H = \mathcal{G}_O(\mathcal{N})$; $B = A(H)$ is the O-algebra of H given in notation of n.3.2 as $O[X_1, \dots, X_u]$ with the equations $X_i^p - \eta_i \sum_j X_j c_{ji} = 0, \quad 1 \leqslant i \leqslant u$. Here $(c_{ij}) \in \mathrm{GL}_u(O)$, all $\eta_i \in O_0$ and $\eta_i | p$. The comultiplication of H appears as a unique O-algebra morphism Δ from B to $B \otimes_O B$ such that $\Delta(X_i) = X_1 \otimes 1 + 1 \otimes X_i + j_i$, where all $j_i \in \mathcal{J}_B \subset I^{DP}_{B\otimes B}$. Here the ideal $\mathcal{J}_B$ is generated by the elements $\tilde{\eta}_i X_i^r \otimes X_i^{p-r}$, where $1 \leqslant i \leqslant u$, $0 < r < p$ and $\tilde{\eta}_i = -p/\eta_i$.

• i will be always an index such that $1 \leqslant i \leqslant u$; $\underline{i}$ will be always a multi-index $(i_1, \dots, i_u)$, where $0 \leqslant i_1, \dots, i_u < p$; an index i can be considered as a special case of the multi-index $(\delta_{i1}, \dots, \delta_{iu})$, where δ is the Kronecker symbol; $r(\underline{i}) = i_1 + \ldots + i_u$;

• $\bar{O} = O_{\bar{K}}$, $\bar{\mathfrak{m}}$ is the maximal ideal in $\bar{O}$; $\bar{B} = B \otimes_O \bar{O}$, $I_{\bar{B}} = I_B \otimes_O \bar{O}$, $\mathcal{J}_{\bar{B}} = \mathcal{J}_B \otimes_O \bar{O}$;

• we use the generators $X_1, \dots, X_u$ for $\bar{B}$ and the generators $X_1 \otimes 1, \dots, X_u \otimes 1, 1 \otimes X_1, \dots, 1 \otimes X_u$ for $\bar{B} \otimes \bar{B}$ to define for any $\alpha \in \bar{O}$, the ideals $I_{\bar{B}}(\alpha)$ and $I_{\bar{B}\otimes\bar{B}}(\alpha)$ in the same way as we defined in 3.3 for $\alpha \in O$, the ideals $I_B(\alpha)$ and $I_{B\otimes B}(\alpha)$. We set for any $\alpha \in \bar{O}$, $I_B(\alpha) = I_{\bar{B}}(\alpha) \cap B$ and similarly, $I_{B\otimes B}(\alpha) = I_{\bar{B}\otimes\bar{B}}(\alpha) \cap (B \otimes B)$;

• any element of $\bar{B}$ can be uniquely written as an $\bar{O}$-linear combination of all $X^{\underline{i}} = X_1^{i_1} \dots X_u^{i_u}$ with all multi-indices $\underline{i}$. Similarly, any element of $\bar{B} \otimes \bar{B}$ can be uniquely written as an $\bar{O}$-linear combination of all $X^{\underline{i}_1} \otimes X^{\underline{i}_2}$ with multi-indices $\underline{i}_1, \underline{i}_2$. We shall use the following obvious property for B (and its analogue for $B \otimes B$):

6.1.1) *if $\alpha \in \bar{\mathfrak{m}}$, all $C_{\underline{i}}, D_{\underline{i}} \in \bar{O}$ and $\sum_{\underline{i}} C_{\underline{i}} X^{\underline{i}} \equiv \sum_{\underline{i}} D_{\underline{i}} X^{\underline{i}} \bmod I_{\bar{B}}(\alpha)$ then for all $\underline{i}$, $C_{\underline{i}} X^{\underline{i}} \equiv D_{\underline{i}} X^{\underline{i}} \bmod I_{\bar{B}}(\alpha)$.*

• in this section we calculate in $\mathrm{m}(I_{\bar{B}})$ and $\mathrm{m}(I_{\bar{B}\otimes\bar{B}})$, which are provided with the Lubin-Tate addition cf. 4.5; one must bear in mind the following agreement: if say, $a \in I_{\bar{B}}$ and it appears in the form $[a]$ then a must be always considered as an element of $\mathrm{m}(I_{\bar{B}})$;

• as earlier, we introduce $O' = O[\pi']$, where $\pi'^p = \pi$; all appropriate extensions of scalars from O to O' will have the dashed notation, eg. $B' = B \otimes_O O'$, $I_{B'}$, $\mathcal{J}_{B'}$ and so on.

Main Lemma. *Suppose $\tilde{\lambda} \in O$, $\tilde{\lambda}^{p-1}|p$. Suppose $f \in \mathrm{m}(I_{\bar{B}})$ and $\delta_{\mathrm{LT}}(f) \in \tilde{\lambda} I_{B\otimes B}$. Then there are*

— *$f_0 \in \tilde{\lambda} I_B$;*
— *for all i and $0 \leqslant l < p$, $o'_{il} \in \pi'^l O$;*
— *for all $\underline{i}$, $D_{\underline{i}} \in \bar{O}$*

such that all $o'^p_{il} \in \tilde{\lambda} O$, $D_i X_i \in I_{\bar{B}}(p)$ and

$$f = [f_0] + \sum_{\substack{0\leqslant l<p\\ 1\leqslant i\leqslant s}} [o'_{il} X_i] + \sum_{1\leqslant i\leqslant s} [D_i X_i] + \left[p \sum_{r(\underline{i})\geqslant 2} D_{\underline{i}} X^{\underline{i}} \right] \bmod p^2 I_{\bar{B}}. \tag{6.1.2}$$

The Main Lemma will be proved in subsections 6.2-6.6 below.

Remark. We need this lemma to study the extensions $G \in \mathrm{Ext}_{\mathrm{Gr}_O}(H, G_{\tilde{\lambda}})$. By Proposition 5.5.4 such extensions appear from elements $f \in \mathcal{H}_{\mathrm{LT}}$ satisfying the conditions of our lemma. On the other hand, we expect that the O-algebra $A(G)$ can be obtained (at least over O') via the special construction from Section 3. The Main Lemma shows that we can replace f by $[f] - [f_0]$, which gives rise to the same extension G. Then in Section 7 we show that these special elements from $\mathcal{H}_{\mathrm{LT}}$ give rise to special extensions constructed in Section 3.

6.2. *Auxiliary lemmas.*

Lemma 6.2.1. *Suppose $C_1, \dots, C_u \in \bar{O}$, $g \in \mathrm{m}(I_{\bar{B}})$, and there is $\beta_0 \in \bar{\mathfrak{m}}$ such that $g \equiv \sum_i [C_i X_i] \bmod I_{\bar{B}}(\beta_0)$. Then there are $C'_{\underline{i}} \in \bar{O}$ such that:*

a) *$g = \sum_i [C'_i X_i] + \left[\sum_{r(\underline{i})\geqslant 2} C'_{\underline{i}} X^{\underline{i}} \right]$;*

b) *for all $1 \leqslant i \leqslant u$, it holds $C_i X_i \equiv C'_i X_i \bmod I_{\bar{B}}(\beta_0)$;*

c) *for all multi-indices $\underline{i}$ with $r(\underline{i}) \geqslant 2$, it holds $C'_{\underline{i}} X^{\underline{i}} \in I_{\bar{B}}(\beta_0)$.*

Proof. Because $g \in \mathrm{m}(I_{\bar{B}})$ there is $\alpha_0 \in \bar{\mathfrak{m}}$ such that $g \in I_{\bar{B}}(\alpha_0)$ and we can assume that $I_{\bar{B}}(\alpha_0) \supset I_{\bar{B}}(\beta_0)$. Then all $C_i X_i \in I_{\bar{B}}(\alpha_0)$. Suppose $\beta \in \bar{m}$, $\beta_0|\beta$ and the statement of our lemma is proved modulo $I_{\bar{B}}(\beta)$. (We can start with $\beta = \beta_0$.) Then $g = \sum_{\underline{i}} [C'_{\underline{i}} X^{\underline{i}}] + [a]$, where $a \in I_{\bar{B}}(\beta)$. It is easy to show that such a can be written as $a = \sum_{\underline{i}} D_{\underline{i}} X^{\underline{i}}$, where all $D_{\underline{i}} \in \bar{O}$ and $D_{\underline{i}} X^{\underline{i}} \in I_{\bar{B}}(\beta)$. This implies that $a \equiv \sum_{\underline{i}} [D_{\underline{i}} X^{\underline{i}}] \bmod I_{\bar{B}}(\beta^p)$ and for all multi-indices $\underline{i}$,

$$[C'_{\underline{i}} X^{\underline{i}}] + [D_{\underline{i}} X^{\underline{i}}] \equiv [(C'_{\underline{i}} + D_{\underline{i}}) X^{\underline{i}}] \bmod I_{\bar{B}}(\beta \alpha_0^{p-1}).$$

This proves our lemma modulo $I_{\bar{B}}(\beta \alpha_0^{p-1})$ and the proof can be finished by repeating this procedure. □

Lemma 6.2.2. *Suppose* $0 \leqslant l < p$, $o'_1, o'_2 \in \pi'^l O$, $o'^p_1, o'^p_2 \in \tilde{\lambda}O$. *Then for any* $a \in I_B$, *there is* $b \in I_B$ *such that*

$$[o'_1 a] + [o'_2 a] = [(o'_1 + o'_2)a] + [\tilde{\lambda} b].$$

Proof. Just apply 4.5.1) and use that for $n \geqslant 1$, $\phi_n(o'_1, o'_2) \in O \cap \tilde{\lambda}O' = \tilde{\lambda}O$. □

Lemma 6.2.3. *Suppose* $1 \leqslant i \leqslant u$, $o' \in O'$ *and* $o'^p \in \tilde{\lambda}O$. *Then there is* $a_i \in I_{B\otimes B}$ *such that* $\delta_{\mathrm{LT}}[o'X_i] = [o'j_i] + [\tilde{\lambda}a_i]$.

Proof. $\delta_{\mathrm{LT}}(o'X_i) = [o'(X_i \otimes 1 + 1 \otimes X_i + j_i)] - [o'(X_i \otimes 1)] - [o'(1 \otimes X_i)]$

$$= [o'(X_i \otimes 1 + 1 \otimes X_i)] + [o'j_i] - \sum_{n\geqslant 1} [o'^{p^n} \phi_n(X_i \otimes 1 + 1 \otimes X_i, j_i)]$$

$$-[o'(X_i \otimes 1 + 1 \otimes X_i)] - \sum_{n\geqslant 1} [o'^{p^n} \phi_n(X_i \otimes 1, 1 \otimes X_i)] = [o'j_i] + [\tilde{\lambda}a_i],$$

with some $a_i \in I_{B\otimes B}$ because $o'^{p^n} \in \tilde{\lambda}O$ if $n \geqslant 1$. □

Definition. If $\alpha, \beta \in \bar{O}$ then $I_{\bar{B}}(\alpha, \beta) = I_{\bar{B}}(\alpha)$ if $\alpha|\beta$ and $I_{\bar{B}}(\alpha, \beta) = I_{\bar{B}}(\beta)$ if $\beta|\alpha$. (So, $I_{\bar{B}}(\alpha, \beta) = I_{\bar{B}}(\alpha) + I_{\bar{B}}(\beta)$.) Similarly, define the ideals $I_{\bar{B}\otimes\bar{B}}(\alpha, \beta)$.

Lemma 6.2.4. *Suppose* $CX_i \in I_{\bar{B}}(\alpha)$, *where* $C \in \bar{O}$ *and* $\alpha \in \bar{\mathfrak{m}}$. *Then*

a) $\delta_{\mathrm{LT}}(CX_i) \equiv -[C^p \phi(X_i)] \bmod I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2}, p^p)$;

b) *if* $\alpha = p$ *then* $\delta_{\mathrm{LT}}(CX_i) \equiv$

$$[Cj_i] - [C^p \phi(X_i)] - [C^p \phi(X_i \otimes 1 + 1 \otimes X_i, j_i)] \bmod (pI_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}} + p^2 I_{\bar{B}\otimes\bar{B}}),$$

in particular, $\delta_{\mathrm{LT}}(CX_i) \in \mathcal{J}_{\bar{B}} + pI_{\bar{B}\otimes\bar{B}}$.

Proof. First, notice that

$$\delta_{\mathrm{LT}}(CX_i) = [C(X_i \otimes 1 + 1 \otimes X_i + j_i)] - [CX_i \otimes 1] - [1 \otimes CX_i]$$

$$= [C(X_i \otimes 1 + 1 \otimes X_i)] + [Cj_i] - [C^p \phi(X_i \otimes 1 + 1 \otimes X_i, j_i)]$$

$$- \sum_{n\geqslant 2} [C^{p^n} \phi_n(X_i \otimes 1 + 1 \otimes X_i, j_i)] - [C(X_i \otimes 1 + 1 \otimes X_i)]$$

$$-[C^p \phi(X_i)] - \sum_{n\geqslant 2} [C^{p^n} \phi_n(X_i \otimes 1, 1 \otimes X_i)].$$

In the case a), the condition $CX_i \in I_{\bar{B}}(\alpha)$ implies that all terms from the above both sums belong to $I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2})$. It remains to note that $C^p \phi(X_i \otimes 1 + 1 \otimes X_i, j_i)$ and Cj_i belong to $I_{\bar{B}\otimes\bar{B}}(p^p)$, because $j_i \in I_{\bar{B}\otimes\bar{B}}(p^p)$.

In the case b), $CX_i \in I_{\bar{B}}(p)$ implies that for all $n \geqslant 2$,

$$C^{p^n} \phi_n(X_i \otimes 1, 1 \otimes X_i) \in p^{p-1} I_{\bar{B}\otimes\bar{B}}.$$

Indeed, ϕ_n is homogeneous of degree p^n and is a linear combination of terms $X_i^{s_1} \otimes X_i^{s_2}$ with $s_1 + s_2 = p^n$. If $n \geqslant 2$ then we can apply to any such term at least $p - 1$ times the relation $C^p X_i^p \in pI_{\bar{B}}$.

For $n \geqslant 2$, we have also that

$$C^{p^n} \phi_n(X_i \otimes 1 + 1 \otimes X_i, j_i) \in pI_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}}.$$

Indeed, we can use that $j_i^p \in p\mathcal{J}_{\bar{B}}$ and that for $s > p^n - p \geqslant 2p$, the elements $C^s(X_i \otimes 1 + 1 \otimes X_i)^s$ belong to $pI_{\bar{B}\otimes\bar{B}}$. The lemma is proved. □

Lemma 6.2.5. *If $\alpha \in \bar{\mathfrak{m}}$ and for all $\underline{i}$ with $r(\underline{i}) \geqslant 2$, it holds $C_{\underline{i}} X^{\underline{i}} \in I_{\bar{B}}(\alpha^p)$ then*

$$\delta_{\mathrm{LT}}\left(\sum_{\underline{i}} C_{\underline{i}} X^{\underline{i}}\right) \equiv \sum_{\underline{i}} C_{\underline{i}} \sum_{\underline{j}'+\underline{j}''=\underline{i}} A_{\underline{j}'\underline{j}''} X^{\underline{j}'} \otimes X^{\underline{j}''} \bmod \left(I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2}) + I_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}}\right),$$

where $r(\underline{j}'), r(\underline{j}'') > 0$ and all coefficients $A_{\underline{j}'\underline{j}''} \in \mathbb{Z}_p^*$.

Proof. Notice that the Lubin-Tate group law on $I_{\bar{B}\otimes\bar{B}}(\alpha^p)$ can be replaced modulo $I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2})$ by the usual addition. Then use that for any multi-index $\underline{i}$ with $r(\underline{i}) \geqslant 2$, it holds $\Delta(X^{\underline{i}}) \equiv (X_1 \otimes 1 + 1 \otimes X_1)^{i_1} \dots (X_s \otimes 1 + 1 \otimes X_s)^{i_s} \bmod I_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}}$, where all appropriate binomial coefficients are prime to p. This implies the statement of our lemma. □

Remark 6.2.6. Notice that we've just proved that $\delta^+\left(\sum_{\underline{i}} C_{\underline{i}} X^{\underline{i}}\right)$ (where $r(\underline{i}) \geqslant 2$) is congruent modulo the ideal $I_{\bar{B}\otimes\bar{B}} J_{\bar{B}}$ to the right-hand side of the formula from above Lemma 6.2.5 .

6.3. *Step 1.*

Suppose $\alpha \in \bar{\mathfrak{m}}$, $\alpha | p$ is such that the statement of the Main Lemma holds modulo $I_{\bar{B}}(\alpha^p)$ with all $D_i X_i \in I_{\bar{B}}(\alpha)$, i.e.

$$f \equiv [f_\alpha] + \sum_{i,l} [o'_{il} X_i] + \sum_i [D_i X_i] \bmod I_{\bar{B}}(\alpha^p), \tag{6.3.1}$$

where all $D_i X_i \in I_{\bar{B}}(\alpha)$, $f_\alpha \in \tilde{\lambda} I_B$ and all $o'_{il} \in \pi'^l O$ are such that $o'^p_{il} \in \tilde{\lambda} O$. Such α always exists, e.g. we can take $\alpha = \alpha_0^{1/p}$, where $\alpha_0 \in \bar{\mathfrak{m}}$ is such that $f \in I_{\bar{B}}(\alpha_0)$. We are going to prove a similar congruence modulo the smaller ideal $I_{\bar{B}}(\alpha^{p^2}, p^p)$.

Apply Lemma 6.2.1 to $g = [f] - [f_\alpha] - \sum_{i,l} [o'_{il} X_i]$ and $\beta_0 = \alpha^p$. Then $f = [f_\alpha] + \sum_{i,l} [o'_{il} X_i] + \sum_i [C_i X_i] + \left[\sum_{r(\underline{i})\geqslant 2} C_{\underline{i}} X^{\underline{i}}\right]$, where all $C_{\underline{i}} \in \bar{O}$, for all $1 \leqslant i \leqslant u$, it holds $C_i X_i \equiv D_i X_i \bmod I_{\bar{B}}(\alpha^p)$ (and therefore all $C_i X_i \in I_{\bar{B}}(\alpha)$) and for all $\underline{i}$ with $r(\underline{i}) \geqslant 2$, it holds $C_{\underline{i}} X^{\underline{i}} \in I_{\bar{B}}(\alpha^p)$.

Now apply Lemmas 6.2.3-6.2.5 and notice that $\mathcal{J}_{\bar{B}} \subset I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2}, p^p)$. Then the condition $\delta_{\mathrm{LT}}(f) \in \tilde{\lambda} I_{B\otimes B}$ implies that

$$-\sum_i C_i^p \phi(X_i) + \sum_{r(\underline{i})\geqslant 2} C_{\underline{i}} \sum_{\underline{j}'+\underline{j}''=\underline{i}} A_{\underline{j}'\underline{j}''} X^{\underline{j}'} \otimes X^{\underline{j}''} \in \tilde{\lambda} I_{B\otimes B} \bmod I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2}, p^p).$$

Notice that all monomials in the both above sums are different and belong to $\bar{O}^{<p}[X_1 \otimes 1, \dots, X_u \otimes 1, 1 \otimes X_1, \dots, 1 \otimes X_u]$. Due to Remark 6.1.1 this implies the following two facts:

1) for all $1 \leqslant i \leqslant u$, $C_i^p \phi(X_i) \equiv o_i \phi(X_i) \bmod I_{\bar{B}\otimes\bar{B}}(\alpha^{p^2}, p^p)$, where $o_i \in \tilde{\lambda} O$;

2) if $r(\underline{i}) \geqslant 2$ then $C_{\underline{i}} X^{\underline{i}} \equiv o_{\underline{i}} X^{\underline{i}} \bmod I_{\bar{B}}(\alpha^{p^2}, p^p)$, where $o_{\underline{i}} \in \tilde{\lambda} O$.

The first fact implies that $(C_i^p - o_i)^p \eta_i^p \equiv 0 \bmod (\alpha^{p^2}, p^p)$ and, therefore,

$$(C_i^p - o_i)\eta_i \equiv 0 \bmod (\alpha^p, p).$$

Decompose each o_i in the form $o_i \equiv \sum_{0\leqslant l<p} o_{il}''^p \bmod p\tilde{\lambda}$, where for all $0 \leqslant l < p$, $o_{il}'' \in \pi'^l O$. Notice that all $o_{il}''^p \in \tilde{\lambda}O$. Then $(C_i^p - \sum_l o_{il}''^p)\eta_i \equiv 0 \bmod(\alpha^p, p)$ or, equivalently,

$$C_i X_i \equiv \sum_l o_{il}'' X_i \bmod I_{\bar{B}}(\alpha^p, p).$$

Notice that also all $C_i X_i, o_{il}'' X_i \in I_{\bar{B}}(\alpha)$. Let $\sum_l o_{il}'' = o_i'$. Then there are $C_{ij}', C_{ij}'' \in \bar{O}$ such that by 4.5 a),

$$[C_i X_i] - [o_i' X_i] \equiv [(C_i - o_i')X_i] + [\phi(C_i, -o_i')X_i^p] \equiv \sum_j [C_{ij}' X_j] \bmod I_{\bar{B}}(\alpha^{p^2}, p^p)$$

(use that X_i^p is a linear combination of X_j, $1 \leqslant j \leqslant u$, and that all terms in the middle and in the right hand side belong to $I_{\bar{B}}(\alpha^p, p)$) and for similar reasons

$$[o_i' X_i] = \sum_l [o_{il}'' X_i] + \sum_j [C_{ij}'' X_j] \bmod I_{\bar{B}}(\alpha^{p^2}, p^p),$$

where all $C_{ij}' X_i, C_{ij}'' X_j \in I_{\bar{B}}(\alpha^p, p)$. This gives, finally, that

$$\sum_i [C_i X_i] = \sum_{i,l} [o_{il}'' X_i] + \sum_i [D_i' X_i] \bmod I_{\bar{B}}(\alpha^{p^2}, p^p),$$

where all $D_i' \in \bar{O}$ and $D_i' X_i \in I_{\bar{B}}(\alpha^p, p)$.

The fact 2) means that with $\tilde{\lambda} f' = \sum_{r(\underline{i})\geqslant 2} o_{\underline{i}} X^{\underline{i}} \in \tilde{\lambda} I_B$, it holds

$$\sum_{r(\underline{i})\geqslant 2} C_{\underline{i}} X^{\underline{i}} \equiv \tilde{\lambda} f' \bmod I_{\bar{B}}(\alpha^{p^2}, p^p).$$

By Lemma 6.2.4 there is $f'' \in \tilde{\lambda} I_B$ such that

$$f \equiv [f''] + \sum_{i,l} [(o_{il}' + o_{il}'')X_i] + \sum_i [D_i' X_i] \bmod I_{\bar{B}}(\alpha^{p^2}, p^p)$$

and we obtained an analogue of (6.3.1) modulo $I_{\bar{B}}(\alpha^{p^2}, p^p)$ with all $D_i X_i \in I_{\bar{B}}(\alpha^p, p)$.

If $I_{\bar{B}}(\alpha^{p^2}, p^p) = I_{\bar{B}}(\alpha^{p^2})$ repeat this step with α replaced by α^p. Then in finitely many steps we obtain that $I_{\bar{B}}(\alpha^{p^2}, p^p) = I_{\bar{B}}(p^p)$. This means that we proved an analogue of formula (6.3.1) modulo $I_{\bar{B}}(p^p)$ (with all $D_i X_i \in I_{\bar{B}}(p)$).

6.4. *Step 2.*

Suppose $\alpha \in \bar{O}$ is such that $p|\alpha$ and suppose

$$f \equiv [f_\alpha] + \sum_{i,l} [o_{il}' X_i] + \sum_i [D_i X_i] \bmod \left(I_{\bar{B}}(\alpha^p) + pI_{\bar{B}}\right), \tag{6.4.1}$$

where as earlier, $f_\alpha \in \tilde{\lambda} I_B$, for all i and $0 \leqslant l < p$, $o'_{il} \in \pi'^l O$, $o'^p_{il} \in \tilde{\lambda} O$, $D_i \in \bar{O}$ and $D_i X_i \in I_{\bar{B}}(p)$. This congruence holds for $\alpha = p$ by results of n.6.3.

Prove that there is a similar congruence modulo $I_{\bar{B}}(\alpha^{p^2}) + pI_{\bar{B}}$.

Apply Lemma 6.2.1. Then

$$f \equiv [f_\alpha] + \sum_{i,l} [o'_{il} X_i] + \sum_i [C_i X_i] + \left[\sum_{r(\underline{i}) \geqslant 2} C_{\underline{i}} X^{\underline{i}} \right] \bmod pI_{\bar{B}},$$

where all $C_{\underline{i}} \in \bar{O}$, $C_i X_i \equiv D_i X_i \bmod I_{\bar{B}}(p)$ and all terms from the last sum belong to $I_{\bar{B}}(\alpha^p)$. Apply Lemmas 6.2.3-6.2.5. Then

(6.4.2)
$$\sum_{r(\underline{i}) \geqslant 2} C_{\underline{i}} \sum_{\substack{\underline{j}' + \underline{j}'' = \underline{i} \\ r(\underline{j}'), r(\underline{j}'') > 0}} A_{\underline{j}' \underline{j}''} X^{\underline{j}'} \otimes X^{\underline{j}''} \in \tilde{\lambda} I_{B \otimes B} \bmod \left(\mathcal{J}_{\bar{B}} + pI_{\bar{B} \otimes \bar{B}} + I_{\bar{B} \otimes \bar{B}}(\alpha^{p^2}) \right).$$

Lemma 6.4.3. *Suppose* $\sum_{\underline{i}_1, \underline{i}_2} a_{\underline{i}_1 \underline{i}_2} X^{\underline{i}_1} \otimes X^{\underline{i}_2} \in \bar{O}^{<p}[X_1 \otimes 1, \ldots, 1 \otimes X_u]$ *belongs to* $\mathcal{J}_{\bar{B}}$. *If multi-indices* $\underline{i}^0_1, \underline{i}^0_2$ *are such that the total degree of the monomial* $X^{\underline{i}^0_1} \otimes X^{\underline{i}^0_2}$ *is less than* p *in each variable* $X_1, \ldots, X_u$ *then* $a_{\underline{i}^0_1 \underline{i}^0_2} \in p\bar{O}$.

Proof. The elements of $\mathcal{J}_{\bar{B}}$ are $\bar{O}$-linear combinations of the terms $\tilde{\eta}_i (X_i^r \otimes X_i^{p-r}) b$, where $1 \leqslant i \leqslant u$, $1 \leqslant r < p$ and b is a monomial of the form $X^{\underline{j}_1} \otimes X^{\underline{j}_2}$. Such product makes a non-zero contribution to $a_{\underline{i}^0_1 \underline{i}^0_2}$ only if its total degree in X_i will become $< p$. This will be a chance only if X_i^p appears in a left or right side of this tensor product. It remains to notice that $\tilde{\eta}_i X_i^p \in pI_B$. $\square$

The above lemma together with relation (6.4.2) implies that for any $\underline{i}$ with $r(\underline{i}) \geqslant 2$, there is an $o_{\underline{i}} \in \tilde{\lambda} O_1$ such that $C_{\underline{i}} X^{\underline{i}} \equiv o_{\underline{i}} X^{\underline{i}} \bmod \left(I_{\bar{B}}(\alpha^{p^2}) + pI_{\bar{B}} \right)$. Therefore,

$$f \equiv [f_{\alpha^p}] + \sum_{i,l} [o'_{il} X_i] + \sum_i [C_i X_i] \bmod \left(I_{\bar{B}}(\alpha^{p^2}) + pI_{\bar{B}} \right),$$

where $f_{\alpha^p} \in \tilde{\lambda} I_B$ is such that $[f_\alpha] - \left[\sum_{\underline{i}} o_{\underline{i}} X^{\underline{i}} \right] = [f_{\alpha^p}]$.

6.5. *Step 3.*

By repeating the procedure from n.6.4 sufficiently many times we shall obtain

(6.5.1)
$$f = [f_0] + \sum_{i,l} [o'_{il} X_i] + \sum_i [D_i X_i] + [pg],$$

where its ingredients f_0, o'_{il} and D_i satify the requirements of the Main Lemma.

Let $g = \sum_{\underline{i}} A_{\underline{i}} X^{\underline{i}}$ with all $A_{\underline{i}} \in \bar{O}$. It remains to prove that we can get rid of all linear terms $A_i X_i$ in $g \bmod pI_{\bar{B}}$.

Notice that for all indices $1 \leqslant i \leqslant u$,

$$[C_i X_i] + [pA_i X_i] \equiv [(C_i + pA_i) X_i] + [\phi(C_i, pA_i) X_i^p] \bmod p^2 I_{\bar{B}},$$

because for $n \geqslant 2$, $\phi_n(C_i, pA_i)X_i^{p^n} \equiv 0 \bmod p^2$ (use that $C_i^{p^n-1}X_i^{p^n}$ is divisible by $C_i^p X_i^p \in pI_{\bar{B}}$). Notice also that

$$\phi(C_i, pA_i)X_i^p \equiv -pC_i^{p-1}A_iX_i^p \equiv p\sum_j C_{ij}X_j \bmod p^2 I_{\bar{B}},$$

where all $C_{ij} \in \bar{O}$ are divisible by $C_i^{p-1}\eta_i \equiv 0 \bmod p^{1-1/p}$, because $C_i^p\eta_i \equiv 0 \bmod p$. This implies that

$$\sum_i [C_iX_i] + \sum_i [pA_iX_i] \equiv$$

$$\textstyle\sum_i[(C_i+pA_i)X_i]+\sum_{i,j}[pC_{ij}X_j] \equiv \sum_i \left[(C_i + pA_i + p\sum_j C_{ji})X_i\right] \bmod p^{2-1/p}I_{\bar{B}}.$$

This relation implies an analogue of formula (6.5.1) with D_i replaced by $C_i + pA_i + p\sum_j C_{ji}$ and where $g \equiv \sum_{r(\underline{i})\geqslant 2} A_{\underline{i}}X^{\underline{i}} \bmod p^{1-1/p}I_{\bar{B}}$. Repeating this step one time more we shall get a similar congruence for g modulo $pI_{\bar{B}}$, i.e. that a new g will not contain linear terms A_iX_i modulo $pI_{\bar{B}}$.

The Main Lemma is proved. □

6.6. *Application of the Main Lemma.*

Proposition 6.6.1. *Suppose $f \in \mathrm{m}(I_{\bar{B}})$ satisfies the assumptions of the Main Lemma and is given by the corresponding formula (6.1.2). Then for $1 \leqslant i \leqslant u$, there are $o_i \in \tilde{\lambda}O$ such that*

$$\sum_r (D_r + \sum_{0\leqslant l<p} o'_{rl})\tilde{\eta}_i d_{ir} - D_i^p \equiv o_i \bmod p\tilde{\eta}_i.$$

Proof. Via Lemmas 6.2.3-6.2.5 the condition $\delta_{\mathrm{LT}}(f) \in \lambda I_{B\otimes B}$ implies that

(6.6.2)
$$\sum_r \left(\sum_l [o'_{rl}j_r] + [D_rj_r] - [D_r^p\phi(X_r)] - [D_r^p\phi(X_r\otimes 1 + 1\otimes X_r, j_r)]\right) + [p\delta^+ g_0]$$

belongs to $\tilde{\lambda}I_{B\otimes B}$ modulo $pI_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}} + p^2 I_{\bar{B}\otimes\bar{B}}$. We are going to follow the coefficient for $\phi(X_i)$ in this formula written as an element of $\bar{O}^{<p}[X_1\otimes 1, \ldots, 1\otimes X_u]$.

Lemma 6.6.3. *Elements from the ideal $I_{\bar{B}\otimes\bar{B}}\mathcal{J}_{\bar{B}}$ contain the monomials $X_i^j \otimes X_i^{p-j}$, where $1 \leqslant i \leqslant u$ and $1 \leqslant j < p$, with coefficients divisible by p.*

Proof of lemma. It is quite similar to the proof of Lemma 6.4.2. □

Now the proof of our Proposition 6.6.1 can be finished as follows:

— working with formula (6.6.2) modulo the ideal $I_{\bar{B}\otimes\bar{B}}(p^{2p})$ we can find the coefficient for $\phi(X_i)$ modulo $p\tilde{\eta}_i$. Indeed, if $C\phi(X_i) \in I_{\bar{B}\otimes\bar{B}}(p^{2p})$ then $C^p\eta_i^p \equiv 0 \bmod p^{2p}$ and $C \equiv 0 \bmod p\tilde{\eta}_i$;

— if we take relation (6.6.2) modulo $I_{\bar{B}\otimes\bar{B}}(p^{2p})$ we can replace the Lubin-Tate group law by the usual addition, because all terms belong to $I_{\bar{B}\otimes\bar{B}}(p^p)$;

— the term $p\delta^+ g_0$ gives the zero contribution to the coefficient for $\phi(X_i)$ modulo p^2, because of Remark 6.2.6 and above Lemma 6.6.3;

— the term $D_r^p\phi(X_r\otimes 1+1\otimes X_r, j_r)$ gives the zero contribution to the coefficient for $\phi(X_i)$ modulo $p\tilde{\eta}_i$ (apply similar arguments as in the proof of Proposition 3.5.1);

— finally, use Proposition 3.5.1 to find out that the coefficient for $\phi(X_i)$ in (6.6.2) coincides modulo $p\tilde{\eta}_i$ with the left-hand side of the formula from our proposition.

The proposition is proved. □

7. Epimorphic property of $\mathcal{G}^O_{O_0}$.

In this section we use the notation and assumptions about O_0 and O from n.4. As in Section 6 we use $O' = O[\pi']$ where $\pi'^p = \pi$. We are going to prove that for any $G_0 \in \mathrm{Gr}_{O_0}$ there is an $\mathcal{M} \in \mathrm{MF}^e_S$ such that $G_0 = \mathcal{G}^O_{O_0}(\mathcal{M})$ or, equivalently, $G := G_0 \otimes_{O_0} O = \mathcal{G}_O(\mathcal{M})$. Notice that by the Tate-Oort classification of group schemes of order p, [TO], this is true for group schemes of order p. Therefore, we can assume that the order $|G_0|$ of G_0 is bigger than p and the above property holds for all $H_0 \in \mathrm{Gr}_{O_0}$ such that $|H_0| < |G_0|$.

7.1. By results of Section 4 we can replace O_0 by the valuation ring of sufficiently large tamely ramified extension of K_0. Therefore, we can assume the existence of $\tilde{\lambda} \in O_0$ such that $\tilde{\eta} := \tilde{\lambda}^{p-1}$ divides p and if $\eta = -p/\tilde{\eta}$ then $G_0 \in \mathrm{Ext}_{\mathrm{Gr}_{O_0}}(H_0, \mathrm{G}_{0\tilde{\eta}})$. Here $H_0 = \mathrm{Spec}\, B_0 \in \mathrm{Gr}_{O_0}$ and $\mathrm{G}_{0\tilde{\eta}} = \mathcal{G}^O_{O_0}(\mathcal{M}_{\tilde{s}})$, where $\mathcal{M}_{\tilde{s}} \in \mathrm{MF}^e_S$ and $\kappa_{SO}(\tilde{s}^p) = \tilde{\eta} \bmod p$. By inductive assumption there is $\mathcal{N} \in \mathrm{MF}^e_S$ such that $H_0 = \mathcal{G}^O_{O^0}(\mathcal{N})$, where $\mathcal{N} \in \mathrm{MF}^e_S$.

We assume that the structure of $\mathcal{N}$ as an object of the category MF^e_S as well as the structure of the coalgebra $B = B_0 \otimes_{O_0} O$ are given in notation from n.3.2. By enlarging (if necessary) the residue field k we can assume that $\tilde{\lambda}$ and all $\tilde{\eta}_i$, $1 \leqslant i \leqslant u$, are just powers of the uniformising element π_0 of O_0.

Let $\bar{f} \in \mathrm{m}(I_{\bar{B}})$ be such that $G_0 = \Theta_{\mathrm{LT}}(\bar{f})$, cf. 5.5.4. Notice that $\bar{f}$ is defined modulo $\tilde{\lambda} I_{B_0} \cap \mathrm{m}(I_{B_0})$ (with respect to the Lubin-Tate addition) and satisfies the requirements

$$\delta_{\mathrm{LT}}(\bar{f}) \in \tilde{\lambda} I_{B_0\otimes B_0}, \quad [p](\bar{f}) \in \tilde{\lambda}^p I_{B_0}. \tag{7.1.1}$$

Apply the Main Lemma from Section 6 to $\bar{f}$. Then there is $f_0 \in \mathrm{m}(I_B) \cap \tilde{\lambda} I_B$ such that

$$[\bar{f}] \equiv [f_0] + \sum_{\substack{1\leqslant i\leqslant u\\ 0\leqslant l<p}} [o'_{il}X_i] + \sum_{1\leqslant i\leqslant u} [D_iX_i] \bmod pI_{\bar{B}},$$

where all $o'_{il} \in \pi'^l O \subset O'$, $o'^p_{il} \in \tilde{\lambda} O$, $D_i \in \bar{O}$ and $D_iX_i \in I_{\bar{B}}(p)$. By Proposition 6.6.1 for all i,

$$\sum_{1\leqslant r\leqslant u} (D_r + \sum_{0\leqslant l<p} o'_{rl})\tilde{\eta}_i d_{ir} - D_i^p \equiv o_i \bmod p\tilde{\eta}_i, \tag{7.1.2}$$

where all $o_i \in \tilde{\lambda} O$. Notice that $[\bar{f}_1] := [\bar{f}] - [f_0]$ corresponds to $G \in \mathrm{Ext}_{\mathrm{Gr}_O}(H, G_\eta)$ under the map Θ_{LT} from 5.5.4. Also notice that congruences (7.1.2) imply that all $o_i \in \tilde{\eta}_i O$ (use that $D_i^p \equiv 0 \bmod \tilde{\eta}_i$ because $D_iX_i \in I_{\bar{B}}(p)$).

For $1 \leqslant i \leqslant u$ and $0 \leqslant l < p$, introduce $o''_{il} \in \pi'^l O \subset O'$ such that

$$o_i \equiv \sum_l o''^p_{il} \bmod p\tilde{\eta}_i.$$

Clearly, all $o''^p_{il} \in \tilde{\lambda}O \cap \tilde{\eta}_i O$. Set $o_{il} := o'_{il} - o''_{il}$.

Proposition 7.1.3. *There is $h \in \tilde{\lambda}I_B \cap I_B(p)$ such that for $[\bar{f}'] = [\bar{f}_1] - [h]$, it holds*

$$l_{\mathrm{LT}}(\bar{f}') \equiv -\sum_{i,l} o_{il}X_i + \sum_{i,l} l_{\mathrm{LT}}(o_{il}X_i) \bmod pI_{\bar{B}}.$$

Proof. Proceed with the following computation modulo $pI_{\bar{B}}$.

$$l_{\mathrm{LT}}(\sum_i [D_iX_i]) = \sum_i l_{\mathrm{LT}}(D_iX_i) \equiv \sum_i (D_iX_i + D_i^pX_i^p/p)$$

$$\equiv \sum_i D_iX_i - \sum_i \frac{o_iX_i^p}{p} + \frac{1}{p}\sum_{i,r}(D_r + \sum_l o'_{rl})\tilde{\eta}_i d_{ir}X_i^p \equiv$$

$$-\sum_{i,l} o'_{il}X_i - \frac{1}{p}\sum_i o_iX_i^p \equiv -\sum_{i,l} o_{il}X_i - \sum_{i,l} l_{\mathrm{LT}}(o''_{il}X_i).$$

(Use that $D_iX_i \in I_{\bar{B}}(p)$ and $\sum_i \tilde{\eta}_i d_{ir}X_i^p = \sum_i \tilde{\eta}_i d_{ir}\eta_i \sum_j X_j c_{ji} = -pX_r$.)

Therefore,

$$l_{\mathrm{LT}}(\bar{f}_1) \equiv -\sum_{i,l} o_{il}X_i + \sum_{i,l} l_{\mathrm{LT}}([o'_{il}X_i] - [o''_{il}X_i]) \bmod pI_{\bar{B}}.$$

Now note that for all i and l, $[o'_{il}X_i] - [o''_{il}X_i] - [o_{il}X_i] = [h_{il}]$, where

$$h_{il} = \sum_{n \geqslant 1} \left[X_i^{p^n}\phi_n(o'_{il}, o''_{il})\right] \in \tilde{\lambda}I_B \cap I_B(p).$$

Indeed by Lemma 6.2.2, all $h_{il} \in \tilde{\lambda}I_B$ and notice that for all $n \geqslant 1$, $\phi_n(o'_{il}, o''_{il}) \equiv 0 \bmod o''_{il}$ (because $\phi_n(X, 0) = 0$) and $o''_{il}X_i \in I_B(p)$ (because $o''^p_{il} \equiv 0 \bmod \tilde{\eta}_i$).

So, if $[h] = \sum_{i,l}[h_{il}]$ then $h \in \tilde{\lambda}I_B \cap I_B(p)$ and

$$l_{\mathrm{LT}}(\bar{f}') = l_{\mathrm{LT}}([\bar{f}_1] - \sum_{i,l}[h_{il}]) \equiv -\sum_{i,l} o_{il}X_i + \sum_{i,l} l_{\mathrm{LT}}(o_{il}X_i) \bmod pI_{\bar{B}}.$$

The proposition is proved. □

7.2. Let $[g] = [\bar{f}'] - \sum_{i,l}[o_{il}X_i]$. Remind that $B' = B \otimes_O O'$ with the augmentation ideal $I_{B'} = I_B \otimes_O O'$ and $\mathcal{J}_{B'} = \mathcal{J}_B \otimes_O O'$.

Proposition 7.2.1.
a) $[p](g) \equiv -p\sum_{i,l} o_{il}X_i \bmod p^2 I_{B'}$;
b) $\delta_{\mathrm{LT}}(g) \in \tilde{\lambda}^{1/p}\mathcal{J}_{B'} + pI_{B'\otimes B'}$.

Proof. a) In the notation from the proof of proposition 7.1.3 it holds

$$[g] = [\bar{f}'] - \sum_{i,l}[o_{il}X_i] = [\bar{f}_1] - \sum_{i,l}[o'_{il}X_i] + \sum_{i,l}[o''_{il}X_i] = \sum_i [D_iX_i] + \sum_{i,l}[o''_{il}X_i] \in I_{B'}(p).$$

(Use that $[p](\bar{f}_1) \in \tilde{\lambda}^p I_B$.) Therefore, $[p](g) \equiv [g^p] + [pg] \equiv 0 \bmod pI_{B'}$ and $l_{\mathrm{LT}}([p]g) \equiv [p]g \bmod p^2 I_{B'}$. So, by Proposition 7.1.3 it holds

$$l_{\mathrm{LT}}([p]g) = pl_{\mathrm{LT}}(g) \equiv -p\sum_{i,l} o_{il}X_i \bmod p^2 I_{B'}.$$

b) As earlier, let $\delta^+ = \Delta - \mathrm{id}\otimes 1 - 1\otimes \mathrm{id}$. Then

$$l_{\mathrm{LT}}(\delta_{\mathrm{LT}}(g)) = \delta^+ l_{\mathrm{LT}}(g) \equiv -\sum_{i,l} o_{il}\delta^+ X_i \equiv 0 \bmod \left(\tilde{\lambda}^{1/p}\mathcal{J}_{B'} + pI_{B'\otimes B'}\right) \tag{7.2.2}$$

because all $o_{il} \equiv 0 \bmod \tilde{\lambda}^{1/p}$ and $\delta^+ X_i \in \mathcal{J}_B$, cf. Proposition 3.2.3. On the other hand by Lemma 6.2.4

$$\delta_{\mathrm{LT}}(g) \equiv \sum_i [\delta_{\mathrm{LT}}(D_iX_i)] + \sum_{i,l}[\delta_{\mathrm{LT}}(o''_{il}X_i)] \equiv 0 \bmod(\mathcal{J}_{\bar{B}} + pI_{\bar{B}\otimes\bar{B}}).$$

Now notice that $\mathcal{J}_{\bar{B}} + pI_{\bar{B}\otimes\bar{B}} \subset I^{DP}_{\bar{B}\otimes\bar{B}}$, l_{LT} induces a one-to-one transformtion of $I^{DP}_{\bar{B}\otimes\bar{B}}$, $\tilde{\lambda}^{1/p}\mathcal{J}_{B'} + pI_{B'\otimes B'} \subset I^{DP}_{\bar{B}\otimes\bar{B}}$, $l_{\mathrm{LT}}(\tilde{\lambda}^{1/p}\mathcal{J}_{B'}) = \tilde{\lambda}^{1/p}\mathcal{J}_{B'}$ and $l_{\mathrm{LT}}(pI_{B'\otimes B'}) = pI_{B'\otimes B'}$. Therefore, (7.2.2) implies that $\delta_{\mathrm{LT}}(g) \in \tilde{\lambda}^{1/p}\mathcal{J}_{B'} + pI_{B'\otimes B'}$.

The proposition is proved. □

7.3. By results of n.5, $G = \mathrm{Spec}\, A$ where the structure of the O-bialgebra A is uniquely recovered from the following conditions

$$A = B[\theta],\quad [p](\tilde{\lambda}\theta) = [p](\bar{f}') \in \tilde{\lambda}^p I_B,\quad \delta_{\mathrm{LT}}(\tilde{\lambda}\theta) = \delta_{\mathrm{LT}}(\bar{f}') \in \tilde{\lambda} I_{B\otimes B}. \tag{7.3.1}$$

Let $A' = A\otimes_O O'$. Introduce $Y, Z \in I_{A'}$ such that

$$[\tilde{\lambda}^{1/p}Z] = [\tilde{\lambda}\theta] - \sum_{i,l}[o_{il}X_i],\quad \tilde{\lambda}Y = \tilde{\lambda}^{1/p}Z + \sum_{i,l} o_{il}X_i. \tag{7.3.2}$$

(The existence of Y and Z follows from the congruences $o_{il} \equiv 0 \bmod(\tilde{\lambda}^{1/p})$ and $\sum_{i,l}[o_{il}X_i] \equiv \sum_{i,l} o_{il}X_i \bmod \tilde{\lambda} I_{B'}$.)

Proposition 7.3.3.

a) $\delta^+ Z \in I_{A'\otimes A'}(p)^p + \dfrac{p}{\tilde\lambda^{1/p}} I_{A'\otimes A'}$;

b) $-\dfrac{1}{p} Z^p \equiv Y \bmod \dfrac{p}{\tilde\lambda} I_{A'}$.

Proof. By 7.2.1 and 7.3.1 $\delta_{\mathrm{LT}}(\tilde\lambda^{1/p} Z) = \delta_{\mathrm{LT}}(g) \in \tilde\lambda^{1/p} I_{B'\otimes B'}(p)^p + p I_{B'\otimes B'}$. Therefore, the part a) will be implied by the following congruence

$$[\tilde\lambda^{1/p} Z \otimes 1] + [1 \otimes \tilde\lambda^{1/p} Z] \equiv [\tilde\lambda^{1/p}(Z\otimes 1 + 1 \otimes Z)] \bmod \tilde\lambda^{1/p} I_{A'\otimes A'}(p)^p.$$

By 4.5.1) this will follow from the congruences

$$\phi_n(\tilde\lambda^{1/p} Z \otimes 1, 1 \otimes \tilde\lambda^{1/p} Z) = \tilde\lambda^{p^{n-1}} \phi_n(Z\otimes 1, 1\otimes Z) \equiv 0 \bmod \tilde\lambda^{1/p} I_{A'\otimes A'}(p)^p,$$

where $n \geqslant 1$. Because all ϕ_n are homogenious polynomials of degree p^n it will be enough to prove that for all $1 \leqslant r < p$, $\tilde\lambda^{1-1/p} Z^r \otimes Z^{p-r} \in I_{A'\otimes A'}(p)^p$. First, notice that the congruence

$$[p](g) = [p](\tilde\lambda^{1/p} Z) \equiv [\tilde\lambda Z^p] + [p\tilde\lambda^{1/p} Z] \bmod p^2 I_A$$

implies by (7.2.1) that $\tilde\lambda Z^p \in p\tilde\lambda^{1/p} I_{A'}$, or equivalently, $\tilde\lambda^{1/p - 1/p^2} Z \in I_{A'}(p)$. Therefore,

$$\tilde\lambda^{1-1/p} Z^r \otimes Z^{p-r} \in I_{A'\otimes A'}(p)^p$$

and the part a) is proved.

Now we can apply 7.2.1 a) to obtain that

$$-p \sum_{i,l} o_{il} X_i \equiv [p](g) \equiv \tilde\lambda Z^p + p\tilde\lambda^{1/p} Z \bmod p^2 I_{A'}$$

and dividing it by $p\tilde\lambda$ we obtain the part b) of our proposition. □

7.4. Remind that $\operatorname{Spec} B = \mathcal{G}_O(\mathcal{N})$, where $\mathcal{N} \in \mathrm{MF}_S^e$ is given in the notation from n.3.2. Let $S' = S[t']$, where $t'^p = t$ and let $\mathcal{N}' = \mathcal{N} \otimes_S S'$. Then $\mathcal{N}' \in \mathrm{MF}_{S'}^{ep}$ and we can extend the identification $\kappa_{SO} : S \bmod t^{ep} \longrightarrow O \bmod p$ to the identification $\kappa_{S'O'} : S'/t^{ep} S' \longrightarrow O'/pO'$.

For all i and l, let $\alpha_{il} \in S'$ be such that $\kappa_{S'O'}(\alpha_{il} \bmod t^{ep}) = \tilde\lambda^{-1/p} o_{il} \bmod p$.

Then in notation from 1.3 and 3.2 we have the following

Lemma 7.4.1. $\sum_{i,l} \alpha_{il} n_i \in Z_{\tilde s}(\mathcal{N}')$.

Proof. It will be sufficient to prove that for all i and l, $t^e \tilde s^{-1} \alpha_{il} \equiv 0 \bmod \tilde s_i$. Via the identification $\kappa_{S'O'}$ these conditions can be rewritten in the form $\pi^e \tilde\lambda^{-1} o_{il} \equiv 0 \bmod \tilde\eta_i^{1/p}$ or, equivalently,

$$o_{il} \eta_i^{1/p} \equiv 0 \bmod \tilde\lambda. \tag{7.4.2}$$

(Use that $\kappa_{SO}(\tilde s_i \bmod t^{ep}) = \tilde\eta_i^{1/p} \bmod p$ and $\kappa_{SO}(\tilde s \bmod t^{ep}) = \tilde\lambda^{1-1/p} \bmod p$.)

These conditions can be verified as follows. By 7.2.1 it holds

$$[p](\bar{f}') = [p](g) + \sum_{i,l}[p](o_{il}X_i) \equiv \sum_{i,l}[o_{il}^p X_i^p] \bmod p^2 I_B. \tag{7.4.3}$$

Therefore, the relation $[p](\bar{f}') \in \tilde{\lambda}^p I_B$ implies that

$$\sum_{i,l}[o_{il}^p X_i^p] \equiv \sum_{i,l} o_{il}^p X_i^p \equiv 0 \bmod(\tilde{\lambda}^p I_B).$$

(Use that all $o_{il}^p \equiv 0 \bmod \tilde{\lambda}$ and the formulae 4.5.3). Finally, the explicit description of the structure of the O-algebra B from n.3.2 implies that for all i and l, $o_{il}^p \eta_i \equiv 0 \bmod(\tilde{\lambda}^p)$ and congruences (7.4.2) are proved.

The lemma is proved. □

Suppose $\mathcal{M}' = (M'^0, M'^1, \varphi_1) \in \mathrm{Ext}_{\mathrm{MF}_{S'}^{ep}}(\mathcal{N}', \mathcal{M}_{\tilde{s}} \otimes_S S')$ is given by the cocycle $\sum_{i,l} \alpha_{il} n_i$ from above Lemma 7.4.1. Remind that $M'^0 = (N^0 \otimes_S S') \oplus mS'$ and $M'^1 = (N^1 \otimes_S S') + m^1 S'$, where $m^1 = \tilde{s}m + \sum_{i,l} \alpha_{il} n_i$ and $\varphi_1(m^1) = m$.

Clearly, the correspondences $m^1 \mapsto Z \bmod I_{A'}^{DP}$ and $m \mapsto Y \bmod I_{A'}^{DP}$, where Y and Z were introduced in 7.3.2, define a unique $\mathcal{F} \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}', \iota(A'))$ such that $\mathcal{F}|_{\mathcal{N}'}$ coincides with the canonical morphism $\iota_{B'} : \mathcal{N}' \longrightarrow \iota(B')$.

Consider $A_1' \in \mathcal{A}(\mathcal{M}')$ such that $A_1' = B'[Y_1] = B'[Y_1, Z_1]$, where

$$Z_1 = \tilde{\lambda}^{1-1/p} Y_1 + \sum_{i,l}(\tilde{\lambda}^{-1/p} o_{il}) X_i, \quad Z_1^p = -pY_1.$$

Then $G_1' = \mathrm{Spec}\, A_1' = \mathcal{G}_{O'}(\mathcal{M}') \in \mathrm{Gr}_{O'}$.

By Proposition 2.4.1, $\mathcal{F}$ gives rise to a unique O'-algebra morphism $F : A_1' \longrightarrow A'$ such that $\iota_{A_1'} \circ \iota(F) = \mathcal{F}$.

Proposition 7.4.4. *F is an isomorphism of coalgebras.*

Proof. Let Δ' and Δ_1' be the comultiplications on A' and A_1'. Prove that

$$F \circ \Delta' = \Delta_1' \circ (F \otimes F).$$

It will be sufficient to prove that the elements $\iota_{A_1'} \circ \iota(F \circ \Delta')$ and $\iota_{A_1'} \circ \iota(\Delta_1' \circ (F \circ F)$ of $\mathrm{Hom}_{\mathcal{MF}_{S'}}(\mathcal{M}', \iota(A' \otimes A'))$ coincide. Clearly, their restrictions to $\mathcal{N}'$ coincide because $F|_{B'} = \mathrm{id}$. It remains to note that the both maps send m^1 to $(Z \otimes 1 + 1 \otimes Z) \bmod I_{A' \otimes A'}^{DP}$. This follows from $\delta^+ Z_1 \in I_{A_1' \otimes A_1'}^{DP}$ (by the definition of the comultiplication on A_1') and $\delta^+ Z \in I_{A' \otimes A'}^{DP}$ by proposition 7.3.3.

It remains to prove that F is an isomorphism of O'-algebras.

Consider the induced homomorphism of geometric points

$$F^* : G'(\bar{K}) \longrightarrow G_1'(\bar{K}).$$

Then F^* induces the identity map on the common quotient $H'(\bar{K})$ and we have the following two cases:

a) F^* is a group isomorphism;

b) $G'_1(\bar{K}) = \mathrm{G}_{\tilde{\eta}}(\bar{K}) \times \operatorname{Im} F^*$.

In the case a), $F \otimes_{O'} K' : A'_1 \otimes_{O'} K' \longrightarrow A' \otimes_{O'} K'$ is an isomoprhism of K'-algebras and, therefore, F is an embedding of A'_1 into A'. This embedding is the identity map on the common subalgebra B'. Therefore, $F(A'_1) = A'$ because the differentes $\mathcal{D}(A'/B')$ and $\mathcal{D}(A'_1/B')$ coincide. So, F is an isomorphism of O'-algebras.

In the case b), $F(A'_1)$ is an O'-subalgebra in A'. It contains B' and $\mathrm{rk}_{O'} F(A'_1) = \mathrm{rk}_{O'} B'$. Therefore, $F(A'_1) = B'$ because the quotient A'/B' has no O'-tosion. In particular, the elements Y and Z from 7.3.2 belong to $I_{B'} + I^{DP}_{A'}$. This implies that

$$\tilde{\lambda}\theta \in \tilde{\lambda}^{1/p} I_{B'} + \tilde{\lambda}^{1/p} I^{DP}_{A'}, \tag{7.4.5}$$

where $\theta \in A$ was introduced in 7.3.1.

Suppose $g \in \mathrm{G}_{\tilde{\eta}}(O)$, $g \neq 0$. Then $\theta(g) = \lambda v$, where $v \in O^*$, and 7.4.3 implies that

$$\pi^* = \lambda\tilde{\lambda} \in \tilde{\lambda}^{1/p} I^{DP}_{O'} \subset I^{DP}_{O'} = (\pi^*\pi'),$$

where $\pi^* \in O$ is such that $\pi^{*p-1} = -p$. The contradiction.

The proposition is completely proved. □

7.5. It remains to prove that there is an $\mathcal{M} \in \mathrm{MF}^e_S$ such that $\mathcal{M} \otimes_S S' = \mathcal{M}'$.

By Proposition 1.3.5 it will be sufficient to prove that for all i, $(\sum_l \alpha_{il}) \in S \bmod \tilde{s}_i$, or equivalently, for all i and $1 \leqslant l < p$, $\alpha_{il} \equiv 0 \bmod \tilde{s}_i$. Applying the identification $\kappa_{S'O'}$ we can replace these conditions by the following equivalent ones

$$o^p_{il} \equiv 0 \bmod \tilde{\lambda}\tilde{\eta}_i, \tag{7.5.1}$$

where as earlier, $1 \leqslant i \leqslant u$ and $1 \leqslant l < p$.

Remind that we started with $f \in \mathrm{m}(I_{\bar{B}})$ such that $[p](f) \in \lambda^p I_{B_0}$ and for $\bar{f}'$ such that $[\bar{f}'] = [\bar{f}] + [h_1]$, where $[h_1] = [f_0] + [h]$ cf. 7.1.3, we have $[p](\bar{f}') \equiv \sum_{i,l} [o^p_{il} X^p_i] \bmod p^2 I_B$. Now notice that $h_1 \in \tilde{\lambda} I_B$ and, therefore, $h^p_1 \in \tilde{\lambda}^p I_{B_0} \bmod p\tilde{\lambda}\pi$. This implies that

$$\sum_{i,l} [o^p_{il} X^p_i] \in I_{B^0} \bmod p\tilde{\lambda} I_B. \tag{7.5.2}$$

Lemma 7.5.3. *For any i and l, $o^p_{il} \equiv \pi^l \tilde{\lambda} u^0_{il} \bmod p\tilde{\lambda}\pi^l$, where all $u^0_{il} \in O_0$.*

Proof. For all i and l, $o_{il} = \pi'^l u_{il}$ with $u_{il} \in O$. Then $o^p_{il} = \pi^l u^p_{il} \in \tilde{\lambda} O$ implies that all $u^p_{il} \in \tilde{\lambda} O$ and , therefore, $u^p_{il} \equiv \tilde{\lambda} u^0_{il} \bmod p\tilde{\lambda}$, where all $u^0_{il} \in O_0$.

The lemma is proved. □

As earlier, for all i, $X^p_i \equiv \eta_i f^0_i \bmod p\pi I_B$, where all $f^0_i \in I_{B_0}$. Notice also that equations for X_i from n.3.2 imply that the residues of $f^0_1 \bmod \pi, \ldots, f^0_u \bmod \pi$ are linearly independent modulo πI_B. Now we can rewrite condition (7.5.2) in the following form

$$\sum_{i,l} [\pi^l u^0_{il} \eta_i f^0_i] \in I_{B^0} \bmod p\tilde{\lambda} I_B. \tag{7.5.4}$$

Clearly, the terms with $l = 0$ already belong to $I_{B_0} \bmod p\tilde{\lambda} I_B$. Therefore, we can assume that in above relation (7.5.4) the index l varies from 1 to $p-1$.

Suppose the ideal in O, which is generated by all $\pi^l u_{il}^0 \eta_i$, where $1 \leqslant l < p$ and $1 \leqslant i \leqslant u$, equals $\pi^c O$. Therefore, $c \in \mathbb{N}$ and $c \not\equiv 0 \bmod p$. Then the left-hand sum in (7.5.4) belongs to $\pi^c I_B \setminus \pi^{c+1} I_B$. For this reason, it belongs to $I_{B^0} \bmod p\tilde{\lambda} I_B$ if and only if $\pi^c \equiv 0 \bmod p\tilde{\lambda}$. In other words, all $o_{il}^p \eta_i \equiv 0 \bmod p\tilde{\lambda}$ if $l \neq 0$. This gives conditions (7.5.2) because $\eta_i \tilde{\eta}_i = -p$.

So, the existence of $\mathcal{M}$ is proved and this implies that $G = \mathcal{G}_O(\mathcal{M})$.

8. Applications.

In this section we prove

1) that our antiequivalence essentially coincides with Breuil's antiequivalence restricted to the category of group schemes killed by p;

2) a criterion for a finite $\mathbb{F}_p[\Gamma_{K_0}]$-module to be isomorphic to $G_0(\bar{K})$, where $G_0 \in \mathrm{Gr}_{O_0}$;

3) establish via the Fontaine-Wintenberger field-of-norms functor a relation between the Galois modules coming from Faltings's strict modules and the Galois modules of the form $G_0(\bar{K})|_{\Gamma_{K_\infty}}$, where $G_0 \in \mathrm{Gr}_{O_0}$ and

$$K_\infty = K(\{\pi_n \mid n \geqslant 0, \pi_{n+1}^p = \pi_n\});$$

4) that a natural duality in the category MF_S^e is transformed to the Cartier duality in Gr_{O_0} via the functor $\mathcal{G}_{O_0}^O$.

8.1. *Relation to Breuil's antiequivalence.* Denote by $\mathrm{Br}_{O_0}^O : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_{O_0}$ the restriction of Breuil's antiequivalence from [Br1] to our categories. Notice that by [Br2, Theorem 3.1.1] Breuil's category of filtered modules over a suitable divided powers envelope of S can be replaced by MF_S^e. Let $\mathrm{Br}_O : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}_O$ be the extension of scalars of Breuil's functor, i.e. for any $\mathcal{M} \in \mathrm{MF}_S^e$, $\mathrm{Br}_O(\mathcal{M}) = \mathrm{Br}_{O_0}^O(\mathcal{M}) \otimes_{O_0} O$.

For any $G \in \mathrm{Im}\,\mathcal{G}_O (= \mathrm{Im}\,\mathrm{Br}_O)$ introduce $\mathcal{M}(G), \mathcal{M}_{\mathrm{Br}}(G) \in \mathrm{MF}_S^e$ such that $\mathcal{G}_O(\mathcal{M}(G)) = G$ and $\mathrm{Br}_O(\mathcal{M}_{\mathrm{Br}}(G)) = G$. Clearly, $\mathcal{M}$ and $\mathcal{M}_{\mathrm{Br}}$ can be considered as contravariant functors from $\mathrm{Im}\,\mathcal{G}_O$ to MF_S^e.

The essential coincidence of $\mathrm{Br}_{O_0}^O$ and $\mathcal{G}_{O_0}^O$ will be proved in the following form.

Theorem A. *For all $G \in \mathrm{Im}\,\mathcal{G}_O$ there are isomorphisms*

$$f(G) \in \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_{\mathrm{Br}}(G), \mathcal{M}(G)),$$

which are functorial in G, in other words for all $\pi \in \mathrm{Hom}_{\mathrm{Gr}_O}(G, G')$, it holds $\mathcal{M}_{\mathrm{Br}}(\pi) \circ f(G) = f(G') \circ \mathcal{M}(\pi)$.

Proof. Suppose $H \in \mathrm{Im}\,\mathcal{G}_O$. Then its O-algebra $A(H)$ can be presented in the form $O[X_1, \ldots, X_u]/(f_1, \ldots, f_u)$ where the generators f_i, $1 \leqslant i \leqslant u$, of the ideal $(f_1, \ldots, f_u)$ are the left hand sides of equations from the beginning of n.3.2. This O-algebra is syntomic and following [Br1, Lemma 2.3.2] introduce for all $n \geqslant 0$,

$$A(H)_n = O[\pi^{p^{-n}}, X_1^{p^{-n}}, \ldots, X_u^{p^{-n}}]/(f_1, \ldots, f_u)$$

and $A(H)_\infty = \cup_{n\geqslant 0} A(H)_n$. For any flat O-algebra B consider the ideal $B(p) = \{b \in B \mid b^p \in pB\}$ in B and introduce

$$\theta(B) = (B/B(p)^p, B(p)/B(p)^p, \varphi_1) \in \mathcal{MF}_S,$$

where φ_1 is induced for all $b \in B(p)$, by the correspondences $b \mapsto -b^p/p$ and the corresponding S-module structure comes from the identification κ_{SO}. The following proposition is just an adjustment of Lemmas 3.1.6 and 3.1.7 from [Br1] to our situation.

Proposition 8.1.1. *There is a functorial in $G, H \in \operatorname{Im}\mathcal{G}_O$ identification of abelian groups $G(A(H)_\infty) = \operatorname{Hom}_{O-alg}(A(G), A(H)_\infty) = \operatorname{Hom}_{\mathcal{MF}_S}(\mathcal{M}_{\mathrm{Br}}(G), \theta(A(H)_\infty))$.*$\square$

Proposition 8.1.2. *Suppose $G, H \in \operatorname{Im}\mathcal{G}_O$ and $\mathcal{M} \in \mathrm{MF}_S^e$. Then the natural embedding $A(H) \subset A(H)_\infty$ induces the following functorial in G, H and $\mathcal{M}$ identifications*

a) $\operatorname{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \theta(A(H)) = \operatorname{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \theta(A(H)_\infty))$*;*

b) $\operatorname{Hom}_{O-alg}(A(G), A(H)) = \operatorname{Hom}_{O-alg}(A(G), A(H)_\infty)$.

Proof. By Lemma 2.4.1 it will be enough to prove a). Then we can use the description of $A(H)$ from n.3.1. Any element $a' \in A(H)_\infty \bmod A(H)_\infty(p)^p$ appears as a k-linear combination of monomials $P_{\underline{\alpha}} = \pi^{\alpha_0} X_1^{\alpha_1} \dots X_u^{\alpha_u}$, where all $\alpha_i \in \mathbb{N}[1/p] \cup \{0\}$ and if the monomial $P_{\underline{\alpha}}$ appears with a non-zero coefficient then $P_{\underline{\alpha}} \in A(H)(p)$, cf. n.3.3. This implies that $\varphi_1(a') \bmod A(H)_\infty(p)^p$ is a k-linear combination of $\varphi_1(P_{\underline{\alpha}})$ for such monomials $P_{\underline{\alpha}}$. Notice that if for $n \geqslant 1$, $P_{\underline{\alpha}} \in A(H)_n$ then $\varphi_1(P_{\underline{\alpha}}) \in A(H)_{n-1}$. Now the proof can be finished by applying these arguments to the images of elements of M^1, where $\mathcal{M} = (M^0, M^1, \varphi_1)$. $\square$

So, we have a functorial in $G, H \in \operatorname{Im}\mathcal{G}_O$ identification

$$\operatorname{Hom}_{O-alg}(A(G), A(H)) = \operatorname{Hom}_{\mathcal{MF}_S}(\mathcal{M}_{\mathrm{Br}}(G), \theta(A(H))$$

and, therefore, the induced functorial identification of abelian groups

$$\operatorname{Hom}_{O-bialg}(A(G), A(H)) = \operatorname{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_{\mathrm{Br}}(G), \mathcal{M}(H)).$$

Take $H = G$ and denote by $f(G)$ the morphism from $\operatorname{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}_{\mathrm{Br}}, \mathcal{M}(H))$ which corresponds under this identification to the identity morphism $\mathrm{id}_{A(G)}$.

Clearly, $f(G)$ is functorial in G. At the same time, $f(G)$ is an isomorphism in MF_S^e. Otherwise, there is a proper subgroup scheme $G_1 \subset G$ such that the composition of $f(G)$ with the natural projection $A(G) \longrightarrow A(G_1)$ is zero, but the corresponding composition of $\mathrm{id}_{A(G)}$ and the natural projection $A(G) \longrightarrow A(G_1)$ is not equal to the counit morphism $A(G) \longrightarrow O$.

Theorem A is completely proved. $\square$

8.2. *Galois modules $G_0(\bar{K})$ and $G(\bar{K})$ with $G_0 \in \mathrm{Gr}_{O_0}$ and $G \in \operatorname{Im}\mathcal{G}_O$.*

Suppose V is a finite abelian group killed by p and provided with a continuous action of Γ_K. Introduce $T(V) = (T(V)^0, T(V)^1, \varphi_1) \in \mathcal{MF}_S$ such that $T(V)^0 = \operatorname{Hom}^{\Gamma_K}(V, \bar{O}/p\bar{O})$, $T(V)^1 = \operatorname{Hom}^{\Gamma_K}(V, (\pi^e\bar{O})/p\bar{O})$ and φ_1 is induced by the map $a \mapsto -a^p/p$, $a \in \pi^e\bar{O}$. As earlier, the corresponding S-module structures appear via the identification $\kappa_{SO} : S/t^{ep}S \longrightarrow O/pO$.

Let $A(V) = \mathrm{Map}^{\Gamma_K}(V, \bar{O}) \in \mathrm{Aug}_O$ with the augmentation ideal $I_{A(V)} = \{a \in A(V) \mid a(0) = 0\}$. Notice that if $A(V)_K := A(V) \otimes_O K = \mathrm{Map}^{\Gamma_K}(V, \bar{K})$ then $\operatorname{Spec} A(V)_K$ has a natural structure of a finite group scheme over K and V is the Γ_K-module of its $\bar{K}$-points.

Introduce the functor $\iota^{(p)} : \mathrm{Aug}_O \longrightarrow \mathcal{MF}_S$ such that for $A \in \mathrm{Aug}_O$, $\iota^{(p)}(A) = (I_A/I_A(p)^p, I_A(p)/I_A(p)^p, \varphi_1)$, where as usually we use the identification κ_{SO} to provide $I_A/I_A(p)^p$ with an S-module structure (notice that $I_A(p)^p \supset pI_A$) and φ_1 is induced by the correspondence $a \mapsto -a^p/p$, $a \in I_A(p)$. Notice that the embedding $I_A(p)^p \subset I_A^{DP}$ induces a strict epimorphism $\iota_p^{DP} : \iota^{(p)}(A) \longrightarrow \iota^{DP}(A)$ in the category $\mathcal{MF}_S$. Suppose $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ and $A \in \mathcal{A}(\mathcal{M})$. By Proposition 2.3.2, $\theta_A^{DP} : \mathcal{M} \longrightarrow \iota^{DP}(A)$ is φ_1-nilpotent. Then there is a unique morphism $\theta_A^{(p)} \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \iota^{(p)}(A))$ such that $\theta_A^{(p)} \circ \iota_p^{DP} = \theta_A^{DP}$ and $\theta_A^{(p)}$ is φ_1-nilpotent.

Let $G = \mathcal{G}_O(\mathcal{M}) = \operatorname{Spec} A$. Suppose

$$\alpha : V \longrightarrow G(\bar{K}) \in \mathrm{Hom}_{\mathbb{F}_p[\Gamma_K]}(V, G(\bar{K})).$$

Consider the morphism of augmented O-algebras $\alpha^* : A \longrightarrow A(V)$ given by the correspondence $a \mapsto \{a(\alpha(v)) \mid v \in V\}$. Then we obtain the morphism $\alpha_A := \iota^{(p)}(\alpha^*) : \iota^{(p)}(A) \longrightarrow \iota^{(p)}(A(V))$ in the category $\mathcal{MF}_S$. Let $\gamma^{(p)} = \iota^{(p)} \circ \alpha_A : \mathcal{M} \longrightarrow \iota^{(p)}(A(V))$. Then $\gamma^{(p)}(M^0)$ is contained in

$$\{a \in I_{A(V)} \bmod pI_{A(V)} \mid a(v + v') \equiv a(v) + a(v') \bmod p\bar{O}, \forall v, v' \in V\} \subset T^0(V)$$

and $\gamma^{(p)}(M^1)$ is contained in $T^1(V) = \pi^e T^0(V)$. Therefore, $\gamma^{(p)}$ induces a morphism $\gamma : \mathcal{M} \longrightarrow T(V)$ in the category $\mathcal{MF}_S$, and the correspondence $\alpha \mapsto \gamma$ gives a map

$$\mathcal{B} : \mathrm{Hom}_{\mathbb{F}_P[\Gamma_K]}(V, G(\bar{K})) \longrightarrow \mathrm{Hom}_{\mathcal{F}M_S}(\mathcal{M}, T(V)).$$

Proposition 8.2.1. *Suppose $|V| = |G(\bar{K})|$. Then $\mathcal{B}$ induces a bijective map from the subset of isomorphisms in $\mathrm{Hom}_{\mathbb{F}_p[\Gamma_K]}(V, G(\bar{K}))$ to the subset of φ_1-nilpotent morphisms in $\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, T(V))$.*

Proof. Suppose $\alpha : V \longrightarrow G(\bar{K})$ is an isomorphism of $\mathbb{F}_p[\Gamma_K]$-modules. Prove that $\gamma = \mathcal{B}(\alpha)$ is φ_1-nilpotent.

Because γ factors through $\theta_A^{(p)}$ and $\theta_A^{(p)}$ is φ_1-nilpotent it will be sufficient to prove that α_A induces a φ_1-nilpotent morphism on $\theta_A^{(p)}(\mathcal{M}) = (N^0, N^1, \varphi_1) \subset \iota^{(p)}(A)$.

- Prove that $T := \operatorname{Ker} \alpha_A\big|_{\theta_A^{(p)}(\mathcal{M})} \subset N^1$.

Suppose $n_0 \in N^0 \setminus N^1$ and $\alpha_A(n_0) = 0$.

Take $m_0 \in M^0$ such that $\theta_A^{(p)}(m_0) = n_0$; clearly, $n_0 \notin N^1$ implies that $m_0 \notin M^1$.

Because $\mathcal{M} \in \mathrm{MF}_S^e$, we can choose for all $i \geqslant 1$, $s_i \in S$, $m_i^1 \in M^0 \setminus tM^1$ and $m_i \in M^0 \setminus tM^0$ such that $m_i^1 = s_i m_{i-1}$ and $m_i = \varphi_1(m_i^1)$. Set $n_i^1 = s_i n_{i-1}$ and $n_i = \varphi_1(n_i^1)$; clearly, all n_i and n_i^1 belong to $\operatorname{Ker} \alpha_A$.

Notice that all $n_i^1 \notin tN^1$. (Otherwise, there is $m' \in M^1$ such that $m_i^1 - tm' \in \operatorname{Ker} \theta_A^{(p)}$, but $\operatorname{Ker} \theta_A^{(p)} \subset tM^1$ because $\theta_A^{(p)}$ is φ_1-nilpotent, cf. 1.2.3, and, therefore, $m_i' \in tM^1$.) In particular, all n_i^1 and n_i are not equal to zero.

Let $f_0 \in I_A$ be such that $f_0 \bmod I_A(p)^p = n_0$. For $i \geqslant 1$, choose $o_i \in O$ such that $\kappa_{SO}(s_i \bmod t^{ep}) = o_i \bmod p$, and then by induction on i choose $f_i \in I_A$, $f_i^1 \in I_A(p)$

such that $f_i^1 = o_i f_{i-1}$ and $f_i = -(f_{i-1}^1)^p/p$. Then all $f_i \notin pI_A \subset I_A(p)^p$, because $f_i \bmod I_A(p)^p = n_i \neq 0$. On the other hand, $\alpha_A(n_0) = 0$ implies that $f_0 \in pA(V)$. Therefore, all $f_i \in p^{c_i}A(V)$, where $c_i = p^i - (1 + p + \cdots + p^{i-1}) \to +\infty$ if $i \to \infty$. This implies the existence of $i_0 \in \mathbb{N}$ such that $f_{i_0} \in pI_A$ and, therefore, $n_{i_0} = 0$. The contradiction.

- Prove that $\varphi_1|_T$ is nilpotent.

First, $\varphi_1(T) \subset T$ because α_A commutes with φ_1.

Now suppose $n_0 \in T$. Then there is $f_0 \in I_A(p) \cap pA(V)$ such that $f_0 \bmod I_A(p)^p = n_0$. Define by induction on $i \geqslant 1$, $n_i \in T$ and $f_i \in I_A(p)$ such that $n_i = \varphi_1(n_{i-1})$ and $f_i = -f_{i-1}^p/p$. (Notice that $n_i \in T$ because $\varphi_1(T) \subset T$, and $f_i \in I_A(p)$ because $f_i \bmod I_A(p)^p = n_i$.) As earlier, $f_0 \in pA(V)$ implies that $f_i \in p^{c_i}A(V)$ where $c_i \to +\infty$ if $i \to \infty$. Therefore, there is an $i_0 \in \mathbb{N}$ such that $f_{i_0} \in pI_A$ and $n_{i_0} = 0$. So, $\gamma = \mathcal{B}(\alpha)$ is φ_1-nilpotent.

Now suppose there is a φ_1-nilpotent morphism $\gamma : \mathcal{M} \longrightarrow T(V)$ in the category $\mathcal{MF}_S$.

Let $\bar{A}(V) = \mathrm{Map}(V, \bar{O}) \in \mathrm{Aug}_{\bar{O}}$ with $I_{\bar{A}(V)} = \{a \in \bar{A}(V) \mid a(0) = 0\}$. Then the natural embedding of $T(V)$ into $\iota^{(p)}(\bar{A}(V)) = (I_{\bar{A}(V)}/pI_{\bar{A}(V)}, \pi^e I_{\bar{A}(V)}/pI_{\bar{A}(V)}, \varphi_1)$ allows us to consider γ as a φ_1-nilpotent morphism from $\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, \iota^{(p)}(\bar{A}(V)))$. If $A \in \mathcal{A}(\mathcal{M})$ then by Proposition 2.4.1 there is a unique morphism of augmented $\bar{O}$-algebras $\bar{\mathcal{F}} : A \otimes_O \bar{O} \longrightarrow \bar{A}(V)$, which corresponds to the composition γ^{DP} of γ and $\iota_p^{DP} : \iota^{(p)}(\bar{A}(V)) \longrightarrow \iota^{DP}(\bar{A}(V))$.

Then:

a) because $T(V)$ is Γ_K-invariant in $\iota^{(p)}(\bar{A}(V))$, $\bar{\mathcal{F}} = \mathcal{F} \otimes_O \bar{O}$, where $\mathcal{F} \in \mathrm{Hom}_{\mathrm{Aug}_O}(A, A(V))$;

b) because $T^0(V) \subset \mathrm{Hom}(V, \bar{O} \bmod p)$, $\bar{\mathcal{F}}_K = \bar{\mathcal{F}} \otimes_{\bar{O}} \bar{K}$ is a morphism of $\bar{K}$-coalgebras $A \otimes_O \bar{K} \longrightarrow \mathrm{Map}(V, \bar{K})$.

The above properties a) and b) imply that $\mathcal{F}_K = \mathcal{F} \otimes_O K$ is a morphism of K-bialgebras $A_K = A \otimes_O K \longrightarrow A(V) \otimes_O K = \mathrm{Map}^{\Gamma_K}(V, \bar{K})$.

Let $B := \mathcal{F}(A) \subset A(V)$ with the induced structure of augmented O-algebra. Then B is a flat O-algebra and, if $\Delta_V : A(V) \longrightarrow A(V \times V) \supset A(V) \otimes_O A(V)$ is induced by the addition $V \times V \longrightarrow V$, then $\Delta_V(B) \subset B \otimes_O B$. This implies that $H = \mathrm{Spec}\, B$ has the induced structure of an object of the category Gr_O and $\mathrm{Spec}\, \mathcal{F} : H \longrightarrow G$ is a closed embedding in Gr_O. Therefore, there is an $\mathcal{N} \in \mathrm{MF}_S^e$ such that $\mathcal{G}_O(\mathcal{N}) = H$ and a strictly epimorphic $f \in \mathrm{Hom}_{\mathrm{MF}_S^e}(\mathcal{M}, \mathcal{N})$ such that $\mathcal{G}_O(f) = \mathrm{Spec}\, \mathcal{F}$. From the definition of f it is clear that $\gamma^{DP} : \mathcal{M} \longrightarrow \iota^{DP}(A(V))$ factors through f and the corresponding morphism $\mathcal{N} \longrightarrow \iota^{DP}(A(V))$ is still φ_1-nilpotent. Therefore, f is an isomorphism in MF_S^e and $\mathcal{F}_K$ is an isomorphism of the K-bialgebra A_K and a K-sub-bialgebra of $\mathrm{Map}^{\Gamma_K}(V, \bar{K})$.

It remains to notice that $\mathrm{rk}_K A_K = p^{\mathrm{rk}_S M^0} = p^{\mathrm{rk}_{\mathbb{F}_p} V} = \mathrm{rk}_K A(V)_K$ implies that $\mathcal{F}_K(A_K) = A(V)_K$. So, $G(\bar{K}) \simeq V$ as $\mathbb{F}_p[\Gamma_K]$-modules. Clearly, if $\mathcal{F}_K$ is induced by the $\mathbb{F}_p[\Gamma_K]$-isomorphism $\alpha : V \longrightarrow G(\bar{K})$ then $\mathcal{B}(\alpha) = \lambda$.

Proposition 8.2 is completely proved. □

We can reformulate it as the following criterion (use results of section 4 for part b)).

Theorem B. a) *A finite $\mathbb{F}_p[\Gamma_K]$-module V is isomorphic to $G(\bar{K})$, where $G \in \mathrm{Im}(\mathcal{G}_O)$, if and only there is an $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ such that* $\dim_{\mathbb{F}_p} V =$

$\mathrm{rk}_S(M^0)$, *and a* φ_1*-nilpotent morphism from* $\mathcal{M}$ *to* $T(V)$ *in the category* $\mathcal{MF}_S$.

b) *A finite* $\mathbb{F}_p[\Gamma_{K_0}]$*-module* V_0 *is isomorphic to* $G_0(\bar{K})$, *where* $G_0 \in \mathrm{Gr}_{O_0}$, *if and only if* $V|_{\Gamma_K}$ *appears in the form* $G(\bar{K})$ *with* $G \in \mathrm{Im}\,\mathcal{G}_O$ *and the ramification subgroup* $\Gamma_{K_0}^{(e^*)}$ *with* $e^* = ep/(p-1)$ *act trivially on* V.$\square$

Remark. 1) Clearly, in part a) of the above Theorem, $G = \mathcal{G}_0(\mathcal{M})$;

2) proposition 8.2.1 is also interesting if K_0 is big enough, e.g. all points of $G \in \mathrm{Gr}_{O_0}$ are defined over K_0; in particular, it allows to retrieve the main results of the paper [Ab1]

8.3. *Group schemes from* Gr_{O_0} *and Faltings's strict modules.*
Remind that (cf. basic notation) $S = k[[t]]$ and $S_0 = k[[t_0]]$ with $t_0 = t^p$.

8.3.1. *Characteristic p analogues of* $\mathcal{G}_O$ *and* $\mathcal{G}_{O_0}^O$.

Suppose $S_{00} = \mathbb{F}_p[\tau_{00}]$ where $\tau_{00} \notin S_0^*$. Then the completion $\hat{S}_{00}$ is a closed subring in S_0 with the residue field $\mathbb{F}_p$ and a uniformising element τ_{00}. Consider the categories $\mathrm{Gr}(S_{00})_{S_0}$ and $\mathrm{Gr}(S_{00})_S$ of finite flat commutative group schemes over S_0 and, resp., S, which are provided with strict action of S_{00} and are killed by the corresponding action of τ_{00}. The general concept of such strict modules was introduced in [Fa] and was studied in details in [Ab4].

As earlier, suppose $\mathcal{K}_0 = \mathrm{Frac}\, S_0$, $\mathcal{K} = \mathrm{Frac}\, S$ and $\mathcal{K}_{00} = \mathrm{Frac}\, \hat{S}_{00}$. Then the ramification index of $\mathcal{K}_0$ over $\mathcal{K}_{00}$ is e. The objects of the category $\mathrm{Gr}(S_{00})_{S_0}$ (it was denoted by $\mathrm{DGr}_1'^*(S_{00})_{S_0}$ in [Ab4]) can be described via the antiequivalence $\mathcal{G}_{S_0}^S : \mathrm{MF}_S^e \longrightarrow \mathrm{Gr}(S_{00})_{S_0}$ as follows (cf. [Ab, 4.5.3], where MF_S^e was denoted by $\mathrm{BR}_1(S_{00})_{S_0}$).

Suppose $\mathcal{M} = (M^0, M^1, \varphi_1) \in \mathrm{MF}_S^e$ is given via an S-basis $\bar{m}^1 = (m_1^1, \dots, m_u^1)$ of M^1, an S-basis $\bar{m} = (m_1, \dots, m_u)$ of M^0 and $U \in M_u(S)$, such that $\varphi_1(\bar{m}^1) = \bar{m}$, $\bar{m}^1 = \bar{m}U$ and U divides the scalar matrix $(t^e\delta_{ij}) \in M_u(S)$. Then we can define the functor $\mathcal{G}_S$ from MF_S^e to $\mathrm{Gr}(S_{00})_S$. By definition, $\mathcal{G}_S(\mathcal{M}) = \mathrm{Spec}\, A = \mathcal{H}$, where $A = S[\bar{X}]$, $\bar{X} = (X_1, \dots, X_u)$ and

$$\bar{X}^{(p)} + \tau_{00}{U^{(p)}}^{-1}\bar{X} = 0.$$

Notice that these equations come from the relation $(\bar{X}U)^{(p)} + \tau_{00}\bar{X} = 0$, which is a complete analogue of the corresponding relation from 2.2. The coalgera structure on A is given via the counit $e : A \longrightarrow S$ such that $e(\bar{X}) = 0$ and the comultiplication $\Delta : A \longrightarrow A \otimes_S A$ such that $\Delta(\bar{X}) = \bar{X} \otimes 1 + 1 \otimes \bar{X}$. Finally, the action $[r] : A \longrightarrow A$ of any $r \in S_{00}$ is uniquely determined by the following conditions $[\tau_{00}](a) = 0$ and $[\alpha](a) = \alpha a$ if $a \in I_A := \mathrm{Ker}\, e$ and $\alpha \in \mathbb{F}_p$. It remains to notice that $\mathcal{H}$ appears already as extension of scalars of S_0-scheme $\mathcal{H}_0$, so in this case the problem of descent to S_0 has a trivial solution and the functor $\mathcal{G}_S$ induces the required functor $\mathcal{G}_{S_0}^S$.

Notice that $A \otimes_S \mathcal{K}$ is an etale $\mathcal{K}$-algebra and it makes sense to introduce the $\Gamma_{\mathcal{K}} = \mathrm{Aut}_{\mathcal{K}}(\bar{\mathcal{K}})$-module $\mathcal{H}(\bar{\mathcal{K}})$ of $\bar{\mathcal{K}}$ points of $\mathcal{H}$.

We can see now that the functor $\mathcal{G}_S$, resp. $\mathcal{G}_{S_0}^S$, is just a simplified characteristic p version of the functor $\mathcal{G}_O$, resp. $\mathcal{G}_{O_0}^O$. Nevertheless, the functors $\mathcal{G}_S$ and $\mathcal{G}_{S_0}^S$ are not still very far from the functors $\mathcal{G}_O$ and $\mathcal{G}_{O_0}^O$. In Theorem C below we prove that for any $\mathcal{M} \in \mathrm{MF}_S^e$, the Galois modules $\mathcal{G}_{S_0}^S(\mathcal{M})(\bar{\mathcal{K}})$ and $\mathcal{G}_{O_0}^O(\mathcal{M})(\bar{K})$ can be

identified via the Fontaine-Wintenberger construction of the field-of-norms functor and even more, they can be uniquely recovered one from another.

Suppose $\bar{S}$ is the valuation ring of $\bar{\mathcal{K}}$. Let $\mathcal{V}$ be a finite $\mathbb{F}_p[\Gamma_{\mathcal{K}}]$-module and $T(\mathcal{V}) = (T(\mathcal{V})^0, T(\mathcal{V})^1, \varphi_1) \in \mathcal{MF}_S$, where $T(\mathcal{V})^0 = \mathrm{Hom}^{\Gamma_{\mathcal{K}}}(\mathcal{V}, \bar{S}/\tau_{00}\bar{S})$, $T(\mathcal{V})^1 = \{a \in T(\mathcal{V})^0 \mid a^p = 0\}$ and $\varphi_1 : T(\mathcal{V})^1 \longrightarrow T(V)^0$ is induced by the map $s \mapsto -s^p/\tau_{00}$, where $s \in t^e\bar{S}$.

The following property can be obtained in the same way as above Theorem B.

Theorem B′. *With the above notation suppose $\mathcal{M} \in \mathrm{MF}_S^e$, $\mathcal{H} = \mathcal{G}_S(\mathcal{M})$ and $|\mathcal{V}| = |\mathcal{H}(\bar{\mathcal{K}})|$. Then $\mathcal{V} \simeq \mathcal{H}(\bar{\mathcal{K}})$ as $\mathbb{F}_p[\Gamma_{\bar{K}}]$-modules if and only if there is a φ_1-nilpotent morphism in* $\mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, T(\mathcal{V}))$. □

8.3.2. *Galois modules $G_0(\bar{K})$ and the field-of-norms functor.*

Consider Fontaine's ring $R = \varprojlim \left(\bar{O}/p\bar{O}\right)_n$, where for $n \geqslant 1$, the connecting morphisms $(\bar{O}/p\bar{O})_{n+1} \longrightarrow (\bar{O}/p\bar{O})_n$ are induced by the p-th power map on $\bar{O}$. Let $R_0 = \mathrm{Frac}\, R$ be the fraction field of R. Then R_0 is a complete algebraicly closed valuation field of characteristic p, the embedding of k into $\bar{O}/p\bar{O}$ induces a canionical embedding of k into R_0. We extend it to the closed embedding of S into R by identifying the uniformising element t of S with $(\pi_n \bmod p)_{n\geqslant 1} \in R$ such that $\pi_1 = \pi$ and for all $n \geqslant 2$, $\pi_n \in \bar{O}$ are such that $\pi_n^p = \pi_{n-1}$. Therefore, $\mathcal{K} = \mathrm{Frac}\, S$ is identified with a closed subfield in R_0 and by the Fontaine-Wintenberger theory of the field-of-norms functor, R_0 coincides with the completion of the algebraic closure of $\mathcal{K}$ in R_0. Notice also that $\mathcal{K}$ is an inseparable extension of $\mathcal{K}_0 = \mathrm{Frac}\, S_0$ of degree p.

On the other hand, the absolute Galois group $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$ acts on R_0 and this allows to identify its subgroup $\Gamma_{K_\infty} = \mathrm{Gal}(\bar{K}/K_\infty)$ with the absolute Galois group $\Gamma_{\mathcal{K}} = \mathrm{Aut}_{\mathcal{K}}(\bar{K})$ of $\mathcal{K}$. Here $K_\infty = \cup_{n\geqslant 0} K_n$ and $K_n = K(\pi_n)$ for all $n \geqslant 0$.

Now notice that:

a) the above embedding $S \subset R$ induces an embedding $\bar{S} \subset R_0$ (where $\bar{S}$ is the valuation ring of the algebraic closure $\bar{\mathcal{K}}$ of $\mathcal{K}$ in R_0) and the identification

$$\kappa_{\bar{S}\bar{O}} : \bar{S}/t^{ep}\bar{S} \longrightarrow R/t^{ep}R = \bar{O}/p\bar{O}$$

(use the projection of R to $(\bar{O}/p\bar{O})_1$), which extends our original identification κ_{SO};

b) with respect to the above identification $\Gamma_{\mathcal{K}} = \Gamma_{K_\infty}$, the identification $\kappa_{\bar{S}\bar{O}}$ is compatible with the action of $\Gamma_{\mathcal{K}}$;

c) suppose $F(T) \in W(k)[T]$ is the minimal monic polynomial for $\pi_0 \in K_0$ over $K_{00} = \mathrm{Frac}\, W(k)$. Then $F(T) = T^e + p(b_1T^{e-1} + \cdots + b_{e-1}T + b_e)$, where all $b_i \in W(k)$ and $b_e \in W(k)^*$. Let

$$\tau_{00} = -t_0^e(\bar{b}_e + \bar{b}_{e-1}t_0 + \cdots + \bar{b}_1 t_0^{e-1})^{-1} \in S_0,$$

where all $\bar{b}_i := b_i \bmod p \in k$. Then $\mathcal{K}_{00} = k[[\tau_{00}]]$ is a closed subfield in $\mathcal{K}_0$ and $\mathcal{K}_0$ is a totally ramified extension of $\mathcal{K}_{00}$ of degree e;

d) suppose $s \in \bar{S}$ and $o \in \bar{O}$ are such that $\kappa_{\bar{S}\bar{O}}(s \bmod t^{ep}) = o \bmod p$; then $s \in t^e\bar{S}$ implies that $o \in \pi^e\bar{O}$ and

$$\kappa_{\bar{S}\bar{O}}\left((-s^p/\tau_{00}) \bmod t^{ep}\right) = (-o^p/p) \bmod p.$$

Indeed, it will be sufficient to verify this formula for $s_0 = t^e$ and $o_0 = \pi^e$; then $-t^{pe}/\tau_{00} = \bar{b}_e + \bar{b}_{e-1}t_0 + \cdots + \bar{b}_1 t_0^{e-1}$ and

$$\kappa_{\bar{S}\bar{O}}(-t^{pe}/\tau_{00} \bmod t^{pe}) = (b_e + b_{e-1}\pi_0 + \cdots + b_1\pi_0^{e-1}) \bmod p = (-\pi^{ep}/p) \bmod p.$$

Theorem C. *Suppose $\mathcal{M} \in \mathrm{MF}^e_S$, $H_0 = \mathcal{G}^O_{O_0}(\mathcal{M})$ and $\mathcal{H}_0 = \mathcal{G}^S_{S_0}(\mathcal{M}) \in \mathrm{Gr}(S_{00})_{S_0}$. Then*

a) *with respect to the field-of-norms identification $\Gamma_{\mathcal{K}_0} = \Gamma_{K_\infty} \subset \Gamma_{K_0}$, the $\Gamma_{\mathcal{K}_0}$-modules $H_0(\bar{K})|_{\Gamma_{K_\infty}}$ and $\mathcal{H}_0(\bar{\mathcal{K}})$ are isomorphic;*

b) *the Γ_{K_0}-module $V_0 = H_0(\bar{K})$ can be uniquely recovered from the $\Gamma_{\mathcal{K}_0}$-module $\mathcal{H}_0(\bar{\mathcal{K}})$.*

Proof. Suppose V is a finite $\mathbb{F}_p[\Gamma_K]$-module and $\mathcal{V} = V|_{\Gamma_{K_\infty}}$ is the $\mathbb{F}_p[\Gamma_{\mathcal{K}}]$-module with respect to our identification $\Gamma_{\mathcal{K}} = \Gamma_{K_\infty}$. Then the embedding

$$\mathrm{Hom}^{\Gamma_K}(V, \bar{O}/p\bar{O}) \longrightarrow \mathrm{Hom}^{\Gamma_{K_\infty}}(V, \bar{O}/p\bar{O})$$

together with the identification $\kappa_{\bar{S}\bar{O}}$ induce the embedding $\omega : T(V) \longrightarrow T(\mathcal{V})$ in the category $\mathcal{MF}_S$.

Now notice that if $V = H(\bar{K})$ then there is a φ_1-nilpotent morphism $\gamma \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, T(V))$. Therefore, for $\mathcal{V} = \mathcal{H}(\bar{\mathcal{K}})$, $\gamma \circ \omega_* \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{M}, T(\mathcal{V}))$ is also φ_1-nilpotent and, therefore, $\mathcal{V} \simeq \mathcal{H}(\bar{\mathcal{K}})$. This proves the part a), because $\Gamma_{\mathcal{K}_0} = \Gamma_{\mathcal{K}} = \mathrm{Aut}_{\mathcal{K}_0}(\bar{\mathcal{K}})$. ($\mathcal{K}$ is purely inseparable over $\mathcal{K}_0$.)

In order to prove b) let $e^* = ep/(p-1)$ and notice that by Fontaine's estimates, the ramification subgroup $\Gamma^{(e^*)}_{K_0}$ acts trivially on V_0 and by estimates from [Ab4], $\Gamma^{(e^*)}_{\mathcal{K}_0}$ acts trivially on $\mathcal{V}_0$.

Therefore, it will be sufficient to prove that the field-of-norms embedding $\Gamma_{\mathcal{K}_0} = \Gamma_{K_\infty} \subset \Gamma_{K_0}$ induces group isomorphism $\Gamma_{\mathcal{K}_0}/\Gamma^{(e^*)}_{\mathcal{K}_0} \simeq \Gamma_{K_0}/\Gamma^{(e^*)}_{K_0}$ or, equivalently, we have the following two properties:

1) $\Gamma^{(e^*)}_{\mathcal{K}_0} = \Gamma_{\mathcal{K}_0} \cap \Gamma^{(e^*)}_{K_0}$;

2) $\Gamma_{K_0} = \Gamma_{\mathcal{K}_0}\Gamma^{(e^*)}_{K_0}$.

Now remind that the ramification theory attaches to any finite extension of complete discrete valuation fields with perfect residue fields $L \supset E$, the Herbrand function $\varphi_{L/E}(x)$, $x \geqslant 0$. One can extend the definition of Herbrand's function for Galois extensions from [Se] by the use of the composition property $\varphi_{L'/E}(x) = \varphi_{L/E}(\varphi_{L'/L}(x))$, where L' contains L and is Galois over E. Alternatively, the Appendix to [De] contains a direct construction of the ramification theory for arbitrary (not necessarily Galois) finite extensions L/E by using E-embeddings of L into a fixed algebraic closure $\bar{E}$ of E. Anyway, such Herbrand's function satisfies the following two propertis:

- if $L_1 \supset L \supset E$ are finite field extensions then for all $x \geqslant 0$,

$$\varphi_{L_1/L}(x) = \varphi_{L/E}(\varphi_{L_1/L}(x));$$

- the ramification subgroup $\Gamma^{(v)}_E$ acts trivially on L if and only if $v > v(L/E)$, where $v(L/E)$ is the value of $\varphi_{L/E}$ at its last edge point. (By definition, $(0,0)$ is always an edge point of Herbrand's function.)

Now notice that for any $n \geqslant 0$,

$$\varphi_{K_{n+1}/K_n}(x) = \begin{cases} x, & \text{if } 0 \leqslant x \leqslant e^* p^n \\ e^* p^n + (x - e^* p^n)/p, & \text{if } x \geqslant e^* p^n \end{cases}$$

Therefore, if

$$\varphi_{K_\infty/K_0}(x) = \lim_{n\to\infty} (\varphi_{K_n/K_{n-1}} \circ \ldots \circ \varphi_{K_1/K_0})(x)$$

then $\varphi_{K_\infty/K_0}(e^*) = e^*$ and by the corresponding property of the field-of-norms functor [Wi, Cor. 3.3.6], it holds $\Gamma_{\mathcal{K}_0}^{(e^*)} = \Gamma_{K_\infty} \cap \Gamma_{K_0}^{(\varphi_{K_\infty/K_0}(e^*))} = \Gamma_{K_\infty} \cap \Gamma_{K_0}^{(e^*)}$. This proves the property 1).

Prove the property 2). Suppose L is the subfield of $\bar{K}$ fixed by $\Gamma_{\mathcal{K}_0}\Gamma_{K_0}^{(e^*)} = \Gamma_{K_\infty}\Gamma_{K_0}^{(e^*)}$. Then L is a finite extension of K_0 in K_∞ and $v(L/K_0) < e^*$. If $L \neq K_0$ then there is an $s \geqslant 0$ such that $LK_s = K_{s+1}$ (use that for all $n \geqslant 0$, $[K_{n+1} : K_n] = p$).

Notice that for all $n \geqslant 1$, $v(K_n/K_0) = e^* + e(n-1)$ (use that $\varphi_{K_n/K_0} = \varphi_{K_n/K_{n-1}} \circ \ldots \circ \varphi_{K_1/K_0}$). Therefore, $s \neq 0$ (otherwise, $LK_0 = L = K_1$ but $v(L/K_0) < v(K_1/K_0) = e^*$). But if $s \geqslant 1$ then

$$e^* + es = v(K_{s+1}/K_0) = \max(v(L/K_0), v(K_s/K_0)) = e^* + e(s-1).$$

The contradiction. So, $L = K_0$ and the property 2) is proved.

Theorem C is completely proved. □

8.3.3. *Full faithfulness of the restriction from Γ_{K_0} to Γ_{K_∞}.*

The above methods can be applied to study a more general situation.

Suppose $\mathcal{C}_{K_0}$ is a full subcategory of the category of finite p-torsion modules with continuous action of Γ_K. Let $\mathrm{M}\Gamma_{K_\infty}$ be the category of Γ_{K_∞}-modules. Then we have the functor $\mathcal{F} : \mathcal{C}_{K_0} \longrightarrow \mathrm{M}\Gamma_{K_\infty}$ of restriction of action Γ_{K_0} to the action of $\Gamma_{K_\infty} \subset \Gamma_{K_0}$. For $n \in \mathbb{N}$, let $\mathcal{C}_{K_0}^{(n)}$ be the full subcategory in $\mathcal{C}_{K_0}$ consisting of modules killed by p^n.

Theorem C′. *Suppose for any $H \in \mathcal{C}_{K_0}^{(1)}$ the ramification subgroups $\Gamma_{K_0}^{(e^*)}$ act trivially on H. Then $\mathcal{F}$ is fully faithful.*

Proof. For $n \in \mathbb{N}$, let $\mathcal{F}^{(n)}$ be the restriction of $\mathcal{F}$ to $\mathcal{C}_{K_0}^{(n)}$. Then we can proceed as in 8.3.2 to deduce from $\Gamma_{K_\infty}\Gamma_{K_0}^{(e^*)} = \Gamma_{K_0}$ that $\mathcal{F}^{(1)}$ is fully faithful. Now notice that for any $H_1, H_2 \in \mathcal{C}_{K_0}$ there is a short exact sequence $0 \longrightarrow \mathrm{Ker}(p\,\mathrm{id}_{H_2}) \longrightarrow H_2 \longrightarrow \mathrm{Im}(p\,\mathrm{id}_{H_2}) \longrightarrow 0$ and we can use a devissage procedure (based on the standard 6-terms $\mathrm{Hom} - \mathrm{Ext}$ exact sequence) to deduce by induction that $\mathcal{F}^{(n)}$ is also fully faithful. □

This theorem can be applied in the following cases:

• if $\mathcal{C}_{K_0}$ is the category of Galois modules $G_0(\bar{K})$ where G_0 is an arbitrary finite flat commutative p-group scheme over O_0 we retrieve Breuil's result [Br3, Theorem 3.4.3];

• if K_0 is unramified over $\mathbb{Q}_p$ then we can apply Theorem C' to the category of all finite subquotients of crystalline $\mathbb{Z}_p[\Gamma_{K_0}]$-modules with Hodge-Tate weights of length $< p$ because of the ramification estimates from [Ab5] (if the above length is $\leqslant p-2$ we retrieve the main result of [Br3] where it is sufficient to use Fontaine's ramification estimates from [Fo5]).

8.4. *Cartier duality.* In this subsection we prove that if $\mathcal{N} \in \mathrm{MF}_S^e$ and $\widetilde{\mathcal{N}} \in MF_S^e$ is its dual (cf. the definition below) then $\mathcal{G}_{O_0}^O(\mathcal{N})$ and $\mathcal{G}_{O_0}^O(\widetilde{\mathcal{N}})$ are Cartier dual group schemes. Clearly, it will be sufficient to verify this over O, i.e. that $G = \mathcal{G}_O(\mathcal{N})$ and $\widetilde{G} = \mathcal{G}_o(\widetilde{\mathcal{N}})$ are Cartier dual. We are going to prove this by constructing a non-degenrate bilinear pairing of group functors $G \times \widetilde{G} \longrightarrow \mu_{p,O}$, where as usually $\mu_{p,O}$ is the constant multiplicative group scheme of order p over O.

Let $-p = \pi_0\varepsilon_0$, where $\varepsilon_0 \subset O_0^*$. Let $\omega_0 \in S_0$ be such that $\kappa_{SO}(\omega_0 \bmod t^{ep}) = \varepsilon_0 \bmod p$. Define the σ-linear morphism $\varphi_1 : t^eS \longrightarrow S$ by the relation $\varphi_1(t^es) = \omega_0\sigma(s)$, $s \in S$. Notice that $\varphi_1(t^e\sigma^{-1}(\omega_0)) = 1$ and $\mathcal{S} = (S, t^eS, \varphi_1) \in \mathrm{MF}_S^e$.

Suppose $\mathcal{N} = (N^0, N^1, \varphi_1) \in \mathrm{MF}_S^e$.

Definition. Let $\widetilde{\mathcal{N}} = (\widetilde{N}^0, \widetilde{N}^1, \varphi_1) \in \mathcal{MF}_S$ be such that

a) $\widetilde{N}^0 = \mathrm{Hom}_S(N^0, S)$;

b) $\widetilde{N}^1 = \{f \in \widetilde{N}^0 \mid f(N^1) \subset t^eS\}$;

c) for any $f \in \widetilde{N}^1$, $\varphi_1(f) \in \widetilde{N}^0$ is such that for any $n \in N^1$, $\varphi_1(f)(\varphi_1(n)) = \varphi_1(f(n))$ (cf. the above definition of $\varphi_1|_S$).

Remarks. 1) The condition c) determines φ_1 uniquely because $\varphi_1(N^1)S = N^0$;

2) one can verify easily that $\widetilde{\mathcal{N}} \in \mathrm{MF}_S^e$;

3) In the above definition $\widetilde{\mathcal{N}} \bmod t^{ep}$ does not depend on a choice of ω_0; therefore, for different choices of ω_0, the corresponding objects $\widetilde{\mathcal{N}} = \widetilde{\mathcal{N}}(\omega_0)$ are related via unique isomorphisms in the category MF_S^e as different φ_1-nilpotent lifts of $\widetilde{\mathcal{N}} \bmod t^{ep}$.

Theorem D. *With the above notation, $\widetilde{H} = \mathcal{G}_O(\widetilde{\mathcal{N}})$ is the Cartier dual to $H = \mathcal{G}_O(\mathcal{N})$.*

Proof. Suppose $\mathcal{N}$ is given in notation similar to those from n.3.1. Then we have

— the vector $n = (n_1, \dots, n_u)$ consisting of elements of an S-basis of M^0;

— for $1 \leqslant i \leqslant u$, there are $\tilde{s}'_i \in S$ such that all $\tilde{s}'_i | t^e$ and the vector $n^1 = (n^1_1, \dots, n^1_u) = (\tilde{s}'_1 n_1, \dots, \tilde{s}'_u n_u)$ consists of elements of an S-basis of N^1;

— there is a matrix $U \in \mathrm{GL}_u(S)$ such that $\varphi_1(n^1) = nU$.

Then one can verify that $\widetilde{\mathcal{N}} = (\widetilde{N}^0, \widetilde{N}^1, \varphi_1)$ can be described via the following data:

— the vector $\tilde{n} = (\tilde{n}_1, \dots, \tilde{n}_u)$ consisting of elements of the S-basis of $\widetilde{N}^0$ which is dual to the basis $n_1, \dots, n_u$ of N^0;

— the vector $\tilde{n}^1 = (\tilde{n}^1_1, \dots, \tilde{n}^1_u) := (s'_1\tilde{n}_1, \dots, s'_u\tilde{n}_u)$ consisting of elements of an S-basis of $\widetilde{N}^1$, where for $1 \leqslant i \leqslant u$, $s'_i = t^e\sigma^{-1}(\omega_0)(\tilde{s}'_i)^{-1}$;

— the relation $\varphi_1(\tilde{n}^1) = \tilde{n}\widetilde{U}$, where $\widetilde{U}^t = U^{-1}$ (here $\widetilde{U}^t$ is the transposed to $\widetilde{U}$ matrix from $\mathrm{GL}_u(S)$).

For $1 \leqslant i \leqslant u$, let $\tilde{\eta}'_i, \eta'_i \in O$ be such that $\kappa_{SO}(\tilde{s}'_i \bmod t^{ep}) = \tilde{\eta}'_i \bmod p$ and $\kappa_{SO}(s'_i \bmod t^{ep}) = \eta'_i \bmod p$. Set $\eta_i = -p/\tilde{\eta}'^p_i$ and $\tilde{\eta}_i = -p/\eta'^p_i$.

Then $A = A(H) = O[X_1, \dots, X_u]$ with the equations $X_i^p = \eta_i \sum_j X_j c_{ji}$, where $1 \leqslant i \leqslant u$ and $C = (c_{ji}) \in \mathrm{GL}_u(O)$ is such that $\kappa_{SO}(U \bmod t^{ep}) = C \bmod p$.

Similarly, $\widetilde{A} = A(\widetilde{H}) = O[\widetilde{X}_1, \dots, \widetilde{X}_u]$ with the equations $\widetilde{X}_i^p = \sum_j \widetilde{X}_j \tilde{c}_{ji}$, where $1 \leqslant i \leqslant u$ and $\widetilde{C} = (\tilde{c}_{ji}) \in \mathrm{GL}_u(O)$ is such that $\kappa_{SO}(\widetilde{U} \bmod t^{ep}) = \widetilde{C} \bmod p$.

Lemma 8.4.1. *Let* $Z = \sum_i X_i \otimes \widetilde{X}_i \in I_{A\otimes\widetilde{A}}$. *Then*

$$Z^p + pZ \equiv 0 \bmod (pI_{A\otimes\widetilde{A}}(p)^p + p^2 I_{A\otimes\widetilde{A}}).$$

Proof. Use that for all $1 \leqslant i \leqslant u$, $\eta_i\tilde{\eta}_i \equiv -p \bmod p^2$, $X_i \otimes \widetilde{X}_i \in I_{A\otimes\widetilde{A}}(p)$ and $C\widetilde{C}^t \equiv E \bmod p$, where E is the unit matrix of order u. □

Let $\widetilde{\mathcal{S}} = (Sm, Sm, \varphi_1) \in \mathrm{MF}^e_S$ be such that $\varphi_1(m) = m$. Then $\mathcal{G}_O(\widetilde{\mathcal{S}}) = \mu_{p,O}$ is the constant multiplicative group scheme of order p over O with the algebra $A(\mu_{p,O}) = O[X]$, $X^p + pX = 0$.

Now notice that the correspondence $m \mapsto Z \bmod I^{DP}_{A\otimes\widetilde{A}}$ determines the morphism $q \in \mathrm{Hom}_{\mathcal{MF}_S}(\mathcal{S}, \iota^{DP}(A\otimes\widetilde{A}))$. Therefore, by Lemma 2.4.1, q is induced by a unique morphism of O-algebras

$$e^* : A(\mu_{p,O}) \longrightarrow A(G) \otimes A(\widetilde{G})$$

Clearly, the definitions of the coalgebra structures on $A(H)$ and $A(\widetilde{H})$ from n.2.4, immediately imply that e^* is co-bilinear. It remains to verify that e^* gives a non-degenerate pairing of group functors.

We can assume that K is so large that all $\bar{K}$-points of group schemes H, $\widetilde{H}$ and $\mu_{p,O}$ are defined over K. Then it will be sufficient to verify that if $\tilde{h}_0 \in \widetilde{H}(O)$ is such that for any $h \in H(O)$,

$$e^*(X)(h, \tilde{h}_0) = e_{\mu_{p,O}}(X) = 0 \tag{8.4.2}$$

then $\tilde{h}_0 = 0$. (Here $e_{\mu_p,O} : A(\mu_{p,O} \longrightarrow O$ is the counit map.)

For all i, denote by $\bar{X}_i \in \mathrm{Hom}(H(O), O/pO)$ the images of $X_i \in A(H) \subset \mathrm{Map}(H(O), O)$ with respect to the natural maps

$$\mathrm{Map}(H(O), O) \longrightarrow \mathrm{Map}(H(O), O/pO) \supset \mathrm{Hom}(H(O), O/pO)$$

(use that $\delta^+ X_i \in I_{A\otimes A}(p)^p$ implies that $\bar{X}_i \in \mathrm{Hom}(H(O), O/pO)$). By the results of n.3.4, the generated by $\bar{X}_i$, $1 \leqslant i \leqslant u$, O-submodule $\mathcal{H}(H)$ in $\mathrm{Hom}(H(O), O/pO)$ can be defined in an invariant way just in terms of the image of the corresponding S-module N^0 in $I_A/I_A(p)^p$. This module can't be too small, for $\pi_0^* \in O$ such that $v_p(\pi_0^*) = 1/(p-1)$, it holds

$$\mathcal{H}(H) \supset \pi_0^* \,\mathrm{Hom}(H(O), O/pO). \tag{8.4.3 }$$

(Use the embedding of O-bialgebras $A(H) \supset A(\mu_{p,O})^{\otimes u}$ and that $\mathcal{H}(\mu_{p,O}^{\times u}) = \pi_0^* \,\mathrm{Hom}(H(O), O/pO)$.)

Lemma 8.4.4.

a) $e^*(X) \equiv Z \bmod (I_{A\otimes\widetilde{A}}(p)^p)$;

b) $e^*(X) \equiv Z + Z' \bmod (I_{A\otimes\widetilde{A}}(p)^{2p-1})$, *where* $Z' \in I_{A\otimes\widetilde{A}}(p)$ *is an* O*-linear combination of the terms* $X_{i_1} \dots X_{i_p} \otimes \widetilde{X}_{i_1} \dots \widetilde{X}_{i_p}$ *for all* $1 \leqslant i_1, \dots, i_p \leqslant u$.

Proof. The part a) follows from Lemma 8.4.1 and b) is obtained from a) and the relation $-e^*(X)^p/p = e^*(X)$. $\square$

Now 8.4.2 and 8.4.4 a) imply that in $\mathrm{Hom}(H(O), O/pO)$ it holds

$$\sum_i \widetilde{X}_i(\tilde{h}_0)\bar{X}_i = 0.$$

Then (8.4.3) implies that all $\widetilde{X}_i(\tilde{h}_0) \equiv 0 \bmod(p/\pi_0^*)$.

If $p \geqslant 5$ then $v_p(\widetilde{X}_i(\tilde{h}_0)) \geqslant (p-2)/(p-1) > 1/(p-1)$ and by Lemma 2.4.1 we can conclude that $\tilde{h}_0 = 0$. In order to finish the proof in general case, just use that for all i, $\widetilde{X}_i(\tilde{h}_0) \in \pi_0^* O$. This imples that, cf. Lemma 8.4.4 b), $Z'(h, \tilde{h}_0) \in p\pi_0^* O$ and, therefore, $\sum_i \widetilde{X}_i(\tilde{h}_0)X_i \in p\pi_0^* \operatorname{Map}(H(O), O)$. Therefore, in $\mathrm{Hom}(H(O), O/pO)$ it holds

$$\sum_i (\widetilde{X}_i(\tilde{h}_0)/\pi_0^*)\bar{X}_i = 0.$$

As earlier, this implies that all $\widetilde{X}_i(\tilde{h}_0)/\pi_0^* \in \pi_0^* O$, therefore, $v_p(\widetilde{X}_i(\tilde{h}_0)) \geqslant 2/(p-1) > 1/(p-1)$ and $\tilde{h}_0 = 0$.

Theorem D is completely proved. $\square$

References

[Ab1] V.Abrashkin, *Group schemes of period p (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 3, 435-459; Engl. transl. in, Math. USSR Izvestiya **20** (1983), no. 3, 411-433.

[Ab2] V.Abrashkin, *Honda systems of group schemes of period p (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 3, 451-484; Engl. transl. in, Math. USSR-Izv. **30** (1988), no. 3, 419-453.

[Ab3] V.Abrashkin, *Group schemes over a discrete valuation ring with small ramification (Russian)*, Algebra i Analiz **1** (1989), no. 1, 60-95; Engl. transl. in, Leningrad Math. J. **1** (1990), no. 1, 57-97.

[Ab4] V.Abrashkin, *Galois modules arising from Faltings's strict modules*, Compos. Math. **142** (2006), no. 4, 867-888.

[Ab5] V.Abrashkin, *Modular representations of the Galois group of a local field and a generalisation of a conjecture of Shafarevich (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **53** (1989), no. 6, 1135-1182; Engl. transl. in, Math. USSR-Izv. **35** (1990), no. 3, 469-518.

[BBM] P.Berthelot, L.Breen, W.Messing, *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1982.x+261 pp., vol. 930.

[Br1] C.Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. **152** (2000), no. 2, 489-549.

[Br2] C.Breuil, *Schemas en groupes et corps des normes (unpublished)* (1998), 13 pages.

[Br3] C.Breuil, *Une application de corps des normes*, Compositio Math. **117** (1999), no. 2, 189-203.

[Br4] C.Breuil, *Integral p-adic Hodge theory*, Algebraic Geometry 2000, Azumino (Hotaka), Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan Tokyo, 2002, p. 51-80.

[BCDT] C.Breuil, B.Conrad, F.Diamond, R.Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 81-124.

[Co] B.Conrad, *Finite group schemes over bases with low ramification*, Compositio Math. **119** (1999), no. 3, 239-320.

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

[Fa] G.Faltings, *Group schemes with strict $\mathcal{O}$-action*, Moscow Math. J. **2** (2002), no. 2, 249-279.

[Fo1] J.-M.Fontaine, *Groupes p-divisibles sur les corps locaux*, Asterisque **47-48** (1977).

[Fo2] J.-M.Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt.*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), A1423-A1425.

[Fo3] J.-M.Fontaine, *Il n'y a pas de variete abelienne sur* $\mathbb{Z}$, Inv. Math. **81** (1985), no. 3, 515-538.

[Fo4] J.-M.Fontaine, *Représentations p-adiques des corps locaux.I.*, The Grothendieck Festschrift, Progr.Math., 87, Birkhauser Boston, Boston, MA, 1990, vol. II, p. 249-309.

[Fo5] J.-M.Fontaine, *Scémas propres et lisses sur Z*, Proceedings of the Indo-French Conference on Geometry (Bombay, 1989), Hindustan Book Agency, Delhi, 1993, p. 43–56.

[Ha] M.Hazewinkel, *Formal groups and applications.*, Pure and Applied Mathematics,vol. 78., Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1978.

[Ki1] M.Kisin, *Moduli of finite flat group schemes, and modularity (to appear in Ann. Math.).*

[Ki2] M.Kisin, *Modularity of 2-adic Barsotti-Tate representations , Preprint.*

[Ki3] M.Kisin, *Crystalline representations and F-crystals*, Algebraic geometry and number theory, Progr. Math., vol. 53, Birkhäuser Boston, Boston, MA, 2006, p. 459-496.

[TO] J.Tate, F.Oort, *Group schemes of prime order*, Ann.Sci. École Norm. Sup. **4** (1970), no. 3, 1-21.

[Ra] M.Raynaud, *Schèmas en groupes de type* $(p, \dots, p)$, Bull.Soc.Math.France **102** (1974), 241-280.

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

[Wi] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. Sci. École Norm. Sup.(4) **16** (1983), no. 1, 59–89.

[Zi] T.Zink, *The display of a formal p-divisible group. Cohomologies p-adiques et applications arithmétiques*, Astérisque **278** (2002), 127-248.

Maths Dept., Durham University, Sci. Laboratories, South Rd., Durham, DH1 3LE, U.K.