THE IMAGE OF THE GALOIS GROUP FOR SOME CRYSTALLINE REPRESENTATIONS

Victor A. Abrashkin

Max-Planck-Gesellschaft zur
Förderung der Wissenschaften e.V.
AG „Algebraische Geometrie und
Zahlentheorie“
Jägerstr. 10-11
10117 Berlin
GERMANY

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI 95-109

THE IMAGE OF THE GALOIS GROUP FOR SOME CRYSTALLINE REPRESENTATIONS

Victor A. Abrashkin

Arbeitsgruppe "Algebraische Geometrie und Zahlentheorie"
Jägerstraße 10/11, Berlin 10117, Germany

0. Introduction.

Let K be the quotient field of Witt vectors ring $W(k)$, where k is an algebraically closed field of characteristic $p > 0$, $\Gamma = \mathrm{Gal}(\bar{K}/K)$.

For $a \in \mathbb{N}$, $a \leq p-1$, denote by $\mathrm{M}\Gamma^{\mathrm{cris}}(a)$ a full subcategory of the category of $\mathbb{Z}_p[\Gamma]$-modules, which consists of Γ-invariant lattices of crystalline $\mathbb{Q}_p[\Gamma]$-modules with Hodge-Tate weights from $[0, a]$. Fontaine-Laffaille theory, c.f. [F-L], gives effective way to study objects of the category $\mathrm{M}\Gamma^{\mathrm{cris}}(a)$ by the functor

$$\mathcal{U} : \mathrm{MF}_f(a) \longrightarrow \mathrm{M}\Gamma^{\mathrm{cris}}(a),$$

where $\mathrm{MF}_f(a)$ is some subcategory of the category of filtered $W(k)$-modules.

In this paper we follow Fontaine's idea from [Fo1] to study the image H of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} U$, where $U \in \mathrm{M}\Gamma^{\mathrm{cris}}(a)$.

Let Γ_{tr} be the Galois group of the maximal tamely ramified extension K_{tr} of K in $\bar{K}$. Fix a section $s : \Gamma_{\mathrm{tr}} \longrightarrow \Gamma$ of the natural projection $\Gamma \longrightarrow \Gamma_{\mathrm{tr}}$. Let U be a free $\mathbb{Z}_p$-module of finite rank h with continuos action of Γ. Then U is a semisimple $\mathbb{Z}_p[s(\Gamma_{\mathrm{tr}})]$-module. Introduce the following two basic assumptions about this module (in fact (2_U) implies (1_U)):

(1_U) *in the isotypical decomposition* $U = \oplus_{\alpha\in\mathcal{I}} U_\alpha$ *all components* U_α *are simple;*

(2_U) *in the isotypical decomposition* $\mathrm{End}_{\mathbb{Z}_p} U = (\mathrm{End}_{\mathbb{Z}_p} U)^{s(\Gamma_{\mathrm{tr}})} \oplus (\oplus_{\alpha\in\mathcal{J}} E_\alpha)$ *all components (with nontrivial action of* $s(\Gamma_{\mathrm{tr}})$*)* E_α *are simple.*

The first assumption implies, that $U \otimes W(\bar{F}_p) = \oplus_{\chi\in S} U_\chi$, where $S = S(U)$ is a finite subset of the group of characters $\mathrm{Char}\,\Gamma_{\mathrm{tr}}$ and $\mathrm{rk}_{W(\bar{\mathbb{F}}_p)} U_\chi = 1$. The set S satisfies the conjugacy condition: $\chi \in S \Rightarrow \sigma\chi \in S$, where σ is absolute Frobenius.

For any such $S \subset \mathrm{Char}\,\Gamma_{\mathrm{tr}}$ consider the set of functions $\mathcal{F}_S$

$$n : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\},$$

such that for any $\chi_1, \chi_2, \chi_3 \in S$

a) $n(\chi_1, \chi_1) \geq 1$;
b) $n(\chi_1, \chi_2) = n(\sigma\chi_1, \sigma\chi_2)$;
c) $n(\chi_1, \chi_2) \leq n(\chi_1, \chi_3) + n(\chi_3, \chi_2)$;

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TeX

d) $n(\chi_1,\chi_1)=\min\{\ n(\chi_1,\chi)+n(\chi,\chi_1)\mid \chi\in S\ \}$.

If U satisfies assumptions (1_U) and (2_U), the function $n_U\in\mathcal{F}_S$ can be defined as follows.

Let H^1 be the image of the higher ramification subgroup $I=\operatorname{Ker}(\Gamma\longrightarrow\Gamma_{\mathrm{tr}})$ in $\operatorname{Aut}_{\mathbb{Z}_p}U$. The Lie $\mathbb{Z}_p$-algebra $\mathcal{H}$ of the p-adic Lie group H^1 is Lie subalgebra and $\mathbb{Z}_p[s(\Gamma_{\mathrm{tr}})]$-submodule of $\operatorname{End}_{\mathbb{Z}_p}U$. If $\alpha\in\mathcal{J}$, then $\mathcal{H}_\alpha=\mathcal{H}\cap E_\alpha=p^{n_\alpha}E_\alpha$ for some $n_\alpha\in\mathbb{Z}_{\geq 0}\cup\{+\infty\}$. If $\chi_1,\chi_2\in S$, $\chi_1\neq\chi_2$, then there exists the unique $\alpha(\chi_1,\chi_2)\in\mathcal{J}$, such that $\chi_1^{-1}\chi_2$ appears as a character of the Γ_{tr}-module $E_{\alpha(\chi_1,\chi_2)}$, and we set

$$n_U(\chi_1,\chi_2)=n_{\alpha(\chi_1,\chi_2)}.$$

If $\chi_1=\chi_2$, set

$$n_U(\chi_1,\chi_1)=\min\{n_U(\chi_1,\chi)+n_U(\chi,\chi_1)\mid \chi\in S(U),\chi\neq\chi_1\ \}.$$

We obtained the function $n_U\in\mathcal{F}_S$, which contains considerable part of information about the image H of Γ in $\operatorname{Aut}_{\mathbb{Z}_p}U$.

One can check up, that for any finite subset $S\subset\operatorname{Char}\Gamma_{\mathrm{tr}}$ (which satisfies the conjugacy condition) and any $n\in\mathcal{F}_S$, there exists Γ-module U (which satisfies assumptions (1_U) and (2_U)), such that $S=S(U)$ and $n=n_U$.

Let $a\in\mathbb{N}$, $a\leq p-1$ and let $(\operatorname{Char}\Gamma_{\mathrm{tr}})(a)$ be union of all $S(U)$, where $U\in\mathrm{M}\Gamma^{\mathrm{cris}}(a)$. Consider standard identification

$$r:\operatorname{Char}\Gamma_{\mathrm{tr}}\longrightarrow R_p'=\{\ r\in\mathbb{Q}\cap[0,1)\mid v_p(r)\geq 0\ \}$$

(if $\chi\in\operatorname{Char}\Gamma_{\mathrm{tr}}$, then $r(\chi)=l/(p^N-1)$, where $0\leq l<p^N-1$, $\chi=\chi_N^{*l}$ and $\chi_N^*\in\operatorname{Char}\Gamma_{\mathrm{tr}}$ is such that $\chi_N^*(\tau)=(\tau\pi_N)\pi_N^{-1}$, where $\pi_N\in\bar{K}$ is such that $\pi_N^{p^N-1}=-p$). Then by Fontaine-Laffaille theory we have

$$r((\operatorname{Char}\Gamma_{\mathrm{tr}})(a))=R_p(a),$$

where $R_p(a)$ consists of $r\in R_p'$, such that all digits $l_s(r), s\geq 0$, of the archimedian expansion "in a base" p

$$r=\frac{l_0(r)}{p}+\dots+\frac{l_s(r)}{p^{s+1}}+\dots$$

belong to $[0,a]$.

Let $a\leq p-2$. In this case the Fontaine-Laffaille functor $\mathcal{U}:\mathrm{MF}_f(a)\longrightarrow\mathrm{M}\Gamma^{\mathrm{cris}}(a)$ is an equivalence of categories. If $U\in\mathrm{M}\Gamma^{\mathrm{cris}}(a)$, then $U=\mathcal{U}(M)$, where $M\in\mathrm{MF}_f(a)$, and our main result (theorem A of n. 2.5.1) gives expression for the function n_U in terms related to the filtered module M.

Let

$$\{\ n_U\mid U\in\mathrm{M}\Gamma^{\mathrm{cris}}(a)\ \}=\bigcup_{S\subset(\operatorname{Char}\Gamma_{\mathrm{tr}})(a)}\mathcal{F}_S'\ .$$

Then by theorem B of n.2.5.2 the subset $\mathcal{F}_S'\subset\mathcal{F}_S$ is given only by one additional condition *d′) if $\chi_1, \chi_0 \in S, r_1 = r(\chi_1), r_0 = r(\chi_0)$ and for all $s \in \mathbb{Z}_{\geq 0}$ one has $l_s(r_0) \geq l_s(r_1)$, then*

$$n(\chi_1, \chi_0) = \min\{ n(\chi_1, \chi) + n(\chi, \chi_0) \mid \chi \in S \}.$$

As application consider the case $a = 1$, $p \geq 3$. If G is a commutative formal group G over $W(k)$ of finite height, then its Tate module $T(G)$ is an object of the category $U \in \mathrm{M}\Gamma^{\mathrm{cris}}(1)$. In this case (under assumptions (1_U) and (2_U)) theorem B gives

$$\mathcal{F}'_{S(T(G))} \neq \mathcal{F}_{S(T(G))} \Leftrightarrow \hat{\mathbb{G}}_m \subsetneq G ,$$

where $\hat{\mathbb{G}}_m$ is the formal multiplicative group. In particular, if G is a 1-dimensional formal group of height h, then

$$r(S(T(G)) = \{ p^i/(p^h - 1) \mid 0 \leq i < h \}$$

and

$$\mathcal{F}'_{S(T(G))} = \mathcal{F}_{S(T(G))}.$$

This equality gives positive answer to the question of J.-M. Fontaine from [Fo1]. In this case the function $n_{T(G)}$ can be also expressed in terms of functional equation for logarithm of G.

We did not consider in this paper the case $a = p - 1$, but it can be considered in the same way using more complicated construction related to some version $\mathcal{U}_1$ of the modification of Fontaine-Laffaille functor from [Ab1]. Then theorem A holds, when $\mathcal{U}$ is replaced by $\mathcal{U}_1$, and theorem B holds (with small correction: if U arises from "connected" filtered module, and the trivial character η belongs to $S(U)$, we must set $r(\eta) = 1$) for all $a \leq p - 1$, so one can apply it also for formal groups in the case $p = 2$.

We did not consider here systematically the second invariant of the image H, which appears as $\mathbb{Z}_p$-module $\mathcal{H} \cap (\mathrm{End}_{\mathbb{Z}_p} U)^{s(\Gamma_{tr})}$. In some cases (e.g. in the case of 1-dimensional formal groups) we prove, that

$$\mathcal{H} \cap (\mathrm{End}_{\mathbb{Z}_p} U)^{s(\Gamma_{tr})} = p(\mathrm{End}_{\mathbb{Z}_p} U)^{s(\Gamma_{tr})},$$

and, therefore, here the knowledge of the function $n_U \in \mathcal{F}_{S(U)}$ is equivalent to the knowledge of the image H of the Galois group Γ.

This paper was written during my stay in the "Arbeitsgruppe Algebraische Geometrie und Zahlentheorie" (Max-Planck-Gesellschaft, Berlin). I express my gratitude to this organization for hospitality.

1. Characterization of some subgroups in $\mathrm{GL}_h(\mathbb{Z}_p)$.

1. Let U be a free $\mathbb{Z}_p$-module of finite rank h. Consider a closed (in p-adic topology) subgroup $H \subset \mathrm{Aut}_{\mathbb{Z}_p} U \simeq \mathrm{GL}_h(\mathbb{Z}_p)$, so one has structure of a continuos $\mathbb{Z}_p[H]$-module on U.

1.1. Consider the following properties C1-C3 of H-module U.

C1. *There is an exact sequence of groups*

$$1 \longrightarrow H^1 \longrightarrow H \longrightarrow H_1 \longrightarrow 1,$$

where H_1 is a cyclic group of order prime to p and H^1 is a pro-p-group.

In this case one can fix a splitting $s : H_1 \longrightarrow H$, what gives the structure of a continuos $\mathbb{Z}_p[s(H_1)]$-module on U. Clearly,

$$U \otimes W(\bar{\mathbb{F}}_p) = \underset{\chi \in S}{\oplus} U_\chi,$$

where $S = S(H)$ consists of characters $\chi \in \mathrm{Hom}(H_1, W(\bar{\mathbb{F}}_p)^*)$, such that

$$U_\chi = \{\ u \in U \otimes W(\bar{\mathbb{F}}_p) \mid hu = \chi(h)u \ \ \forall h \in s(H_1)\ \} \neq 0.$$

If σ is the absolute Frobenius on $W(\bar{\mathbb{F}}_p)$, then one has: $\chi \in S \ \Rightarrow\ \sigma\chi \in S$.

C2. $\mathrm{rk}_{W(\bar{\mathbb{F}}_p)} U_\chi = 1$ *for any $\chi \in S(H)$, i.e. $\mathbb{Z}_p[s(H_1)]$-module U does not contain multiple irreducible components.*

C3. *If $\chi_1, \chi_2, \chi_3, \chi_4 \in S(H)$, $\chi_1 \neq \chi_2$ and $\chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$, then $\chi_1 = \chi_3$ (and, therefore, $\chi_2 = \chi_4$), i.e. $\mathbb{Z}_p[s(H_1)]$-module $\mathrm{End}_{\mathbb{Z}_p} U$ does not contain irreducible multiple components with nontrivial action of $s(H_1)$.*

We prove the following proposition to illustrate these properties.

Proposition. *If the image of H in $\mathrm{Aut}_{\mathbb{F}_p}(U \otimes \mathbb{F}_p)$ is a cyclic group of order $q-1$, where $q = p^h$, then the properties C1-C3 hold and $U_1 = U \otimes \mathbb{F}_p$ is a simple $\mathbb{Z}_p[H]$-module.*

Proof.
Obviously, C1 is true.
Present $S = S(H)$ as a union of σ-orbits

$$S = \{\ \chi_1, \dots, \sigma^{h_1-1}\chi_1; \dots; \chi_s, \dots, \sigma^{h_s-1}\chi_s\ \}.$$

Then $\mathrm{ord}\,\chi_i \mid p^{h_i} - 1$ for $1 \leq i \leq s$, and $h_1 + \dots + h_s = |S| \leq h$. Now

$$q - 1 = C.G.M.\{\ \mathrm{ord}\,\chi_i \mid 1 \leq i \leq s\ \} \leq \prod_{1 \leq i \leq s} (p^{h_i} - 1) \leq p^{h_1 + \dots + h_s} - s$$

gives $s = 1, h_1 + \dots + h_s = h$, or $S = \{\ \chi, \sigma\chi, \dots, \sigma^{h-1}\chi\ \}$ and $\mathrm{ord}\,\chi = q - 1$, what gives the property C2.

Let $\chi_1, \dots, \chi_4 \in S, \chi_1 \neq \chi_2, \chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$. One can assume, that $\chi_1 = \chi, \chi_2 = \sigma^{n_2}\chi, \chi_3 = \sigma^{n_3}\chi, \chi_4 = \sigma^{n_4}\chi$, where $0 \leq n_2, n_3, n_4 < h, n_2 \neq 0$. Because of the property $\mathrm{ord}\,\chi = q - 1$, the equality $\chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$ is equivalent to

$$1 + p^{n_4} \equiv p^{n_2} + p^{n_3} \bmod (q - 1).$$

The both sides of this equivalence are elements from $[2, q]$, so we have the equality

$$1 + p^{n_4} = p^{n_2} + p^{n_3}.$$

Now $n_2 \neq 0 \Rightarrow 1 + p^{n_4} \geq p + 1 > 2 \Rightarrow n_4 \neq 0 \Rightarrow n_3 = 0 \Rightarrow \chi_1 = \chi_3$. So, we have also the property C3.

1.2. Let $\mathcal{H} \subset \mathrm{End}_{\mathbb{Z}_p} U$ be the $\mathbb{Z}_p$-Lie algebra of $H^1 \subset \mathrm{Aut}_{\mathbb{Z}_p} U$. Then $H \mapsto \mathcal{H}$ gives one-to-one correspondence between subgroups $H \subset \mathrm{Aut}_{\mathbb{Z}_p} U$ (with given H_1) and $\mathbb{Z}_p[s(H_1)]$-submodules and topologically nilpotent Lie subalgebras $\mathcal{H}$ of $\mathbb{Z}_p[s(H_1)]$-module and Lie algebra $\mathrm{End}_{\mathbb{Z}_p} U$.

Clearly,

$$\mathrm{End}_{\mathbb{Z}_p} U \subset \mathrm{End}_{W(\bar{\mathbb{F}}_p)}(U \otimes W(\bar{\mathbb{F}}_p)) = \oplus_{\chi_1, \chi_2 \in S} \mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_{\chi_1}, U_{\chi_2}).$$

Under this injection $\mathrm{End}_{\mathbb{Z}_p} U$ consists of

$$(\alpha_{\chi_1,\chi_2})_{\chi_1,\chi_2 \in S} \in \oplus_{\chi_1,\chi_2 \in S} \mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_{\chi_1}, U_{\chi_2}),$$

such that $\sigma\alpha_{\chi_1,\chi_2} = \alpha_{\sigma\chi_1,\sigma\chi_2}$ for any $\chi_1, \chi_2 \in S$, where

$$\sigma\alpha_{\chi_1,\chi_2} : U_{\chi_1^p} \xrightarrow{\sigma^{-1}} U_{\chi_1} \xrightarrow{\alpha_{\chi_1,\chi_2}} U_{\chi_2} \xrightarrow{\sigma} U_{\chi_2^p}.$$

Let η be some character of $s(H_1)$, then
$(\mathrm{End}_{\mathbb{Z}_p} U)_\eta = 0$, if $\eta \neq \chi_1^{-1}\chi_2$ for any $\chi_1, \chi_2 \in S$;
$\mathrm{rk}_{W(\bar{\mathbb{F}}_p)}(\mathrm{End}_{\mathbb{Z}_p} U)_\eta = 1$, if $\eta = \chi_1^{-1}\chi_2$, where $\chi_1, \chi_2 \in S, \chi_1 \neq \chi_2$;
$(\mathrm{End}_{\mathbb{Z}_p} U)^{s(H_1)} = \{\ (\alpha_\chi \,\mathrm{id}_\chi)_{\chi \in S} \mid \alpha_\chi \in W(\bar{\mathbb{F}}_p), \sigma\alpha_\chi = \alpha_{\sigma\chi} \ \ \forall \chi \in S\ \}$.

Now let $\mathcal{H} \otimes W(\bar{\mathbb{F}}_p) = \bigoplus_{\eta \in \mathrm{Char}\, s(H_1)} \mathcal{H}_\eta$. Then the following properties describe $\mathcal{H}$ as a $\mathbb{Z}_p[s(H_1)]$-submodule of $\mathrm{End}_{\mathbb{Z}_p} U$:

a) if $\eta \neq \chi_1^{-1}\chi_2$, where $\chi_1, \chi_2 \in S$, then $\mathcal{H}_\eta = 0$;

b) if $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$, then there exists $n(\chi_1, \chi_2) \in \mathbb{Z}_{\geq 0} \cup \{+\infty\}$, such that

$$\mathcal{H}_{\chi_1^{-1}\chi_2} = p^{n(\chi_1,\chi_2)} \mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_{\chi_1}, U_{\chi_2}).$$

These "integers" $n(\chi_1, \chi_2)$ satisfy the conjugacy condition $n(\chi_1, \chi_2) = n(\sigma\chi_1, \sigma\chi_2)$.

c) $\mathcal{H}_0 = \mathcal{H}^{s(H_1)}$ is some $\mathbb{Z}_p$-submodule of

$$(\mathrm{End}_{\mathbb{Z}_p} U)^{s(H_1)} = \{\ (\alpha_\chi \,\mathrm{id}_\chi)_{\chi \in S} \mid \alpha_\chi \in W(\bar{\mathbb{F}}_p), \sigma\alpha_\chi = \alpha_{\sigma\chi} \ \ \forall \chi \in S\ \}.$$

The following properties describe $\mathcal{H}$ as a topologically nilpotent Lie subalgebra of $\mathrm{End}_{\mathbb{Z}_p} U$:

d) if χ_1, χ_2, χ_3 are different elements of S, then $[\mathcal{H}_{\chi_1^{-1}\chi_2}, \mathcal{H}_{\chi_2^{-1}\chi_3}] \subset \mathcal{H}_{\chi_1^{-1}\chi_3}$ and, therefore, $n(\chi_1, \chi_2) + n(\chi_2, \chi_3) \geq n(\chi_1, \chi_3)$;

e) if $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$, then $[\mathcal{H}_{\chi_1^{-1}\chi_2}, \mathcal{H}_{\chi_2^{-1}\chi_1}] \subset \mathcal{H}_0$ and this means

$$p^{n(\chi_1,\chi_2)+n(\chi_2,\chi_1)}(\mathrm{id}_{\chi_1} - \mathrm{id}_{\chi_2}) \in \mathcal{H}_0 \otimes W(\bar{\mathbb{F}}_p);$$

f) $\mathcal{H}_0 \subset p(\mathrm{End}_{\mathbb{Z}_p} U)^{s(H_1)}$.

If $\chi_1, \chi_2 \in S, \chi_1 \neq \chi_2$, then e) and f) give $n(\chi_1,\chi_2) + n(\chi_2,\chi_1) \geq 1$. So, if we set by definition

$$n(\chi,\chi) = \min\{n(\chi,\chi_2) + n(\chi_2,\chi) \mid \chi_2 \in S, \chi \neq \chi_2 \},$$

and require $n(\chi,\chi) \geq 1$ for all $\chi \in S$, then the above property d) can be reformulated in a following way.

d_1) if $\chi_1, \chi_2, \chi_3 \in S$, then

$$n(\chi_1,\chi_2) + n(\chi_2,\chi_3) \geq n(\chi_1,\chi_3).$$

So, we have

Proposition. *There is one-to-one correspondence between subgroups $H \subset \mathrm{Aut}_{\mathbb{Z}_p} U$, which satisfy the properties C1-C3, and the following data:*

1) *a function $n = n_H : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$, such that for any $\chi_1, \chi_2, \chi_3 \in S$*

$$n(\chi_1,\chi_1) = \min\{n(\chi_1,\chi_2) + n(\chi_2,\chi_1) \mid \chi_2 \in S \} \geq 1;$$

$$n(\sigma\chi_1,\sigma\chi_2) = n(\chi_1,\chi_2);$$

$$n(\chi_1,\chi_2) + n(\chi_2,\chi_3) \geq n(\chi_1,\chi_3);$$

2) *a $\mathbb{Z}_p$-submodule $\mathcal{H}_0 = \mathcal{H}_0(H)$ of $p(\mathrm{End}_{\mathbb{Z}_p} U)^{s(H_1)} \subset p \bigoplus\limits_{\chi \in S} \mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_\chi, U_\chi)$, such that for any $\chi_1, \chi_2 \in S$*

$$p^{n(\chi_1,\chi_2)+n(\chi_2,\chi_1)}(\mathrm{id}_{\chi_1} - \mathrm{id}_{\chi_2}) \in \mathcal{H}_0 \otimes W(\bar{\mathbb{F}}_p).$$

1.3. Consider the following property

C4. *$U_1 = U \otimes \mathbb{F}_p$ is a simple $\mathbb{Z}_p[H]$-module.*

Clearly, C4 implies C2. Under assumption C4 the above description of H can be slightly simplified.

From C1 it follows, that $\mathbb{Z}_p[s(H_1)]$-module U is simple. So, if we fix $\chi \in S = S(H)$, then $S = \{\chi, \sigma\chi, \ldots, \sigma^{h-1}\chi\}$. For $i \in \mathbb{Z}/h\mathbb{Z}$ set $n(i) = n(\sigma^{m_1}\chi, \sigma^{m_2}\chi)$, where $(m_2 - m_1) \bmod h = i$. Then

$$n(i) + n(j) \geq n(i+j),$$

for any $i, j \in \mathbb{Z}/h\mathbb{Z}$. Remark, that $H^1 = H \cap (1 + p\,\mathrm{End}_{\mathbb{Z}_p} U)$, therefore, all $n(i) \in \mathbb{N} \cup \{+\infty\}$, and we obtain the function

$$n = n_{H,\chi} : \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}.$$

To rewrite the condition 2) of proposition of n.1.3, let

$$\mathcal{H} = \oplus_{i \in \mathbb{Z}/h\mathbb{Z}} \mathcal{H}_i,$$

where $\mathcal{H}_0 = \mathcal{H}^{s(H_1)}$ as earlier, and for $i \in \mathbb{Z}/h\mathbb{Z} \setminus \{0\}$ $\mathcal{H}_i$ is an irreducible $\mathbb{Z}_p[s(H_1)]$-module, such that $\mathcal{H}_{i,\chi^{-1}\sigma^i\chi} \neq 0$.

For any $m \in \mathbb{Z}/h\mathbb{Z}$, let $U_{\sigma^m\chi} = W(\bar{\mathbb{F}}_p)e_m$, where $\sigma e_m = e_{m+1}$. For any $m_1, m_2 \in \mathbb{Z}/h\mathbb{Z}$, let $e_{m_1,m_2} \in \mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_{\sigma^{m_1}\chi,\sigma^{m_2}\chi})$ be such that $e_{m_1,m_2}(e_{m_1}) = e_{m_2}$. In this notation for $q = p^h$ and any $i \in \mathbb{Z}/h\mathbb{Z}$

$$\mathcal{H}_i \subset \{ \sum_{m\in\mathbb{Z}/h\mathbb{Z}} \alpha_m e_{m,m+i} \mid \alpha_m \in W(\mathbb{F}_q), \sigma\alpha_m = \alpha_{m+1} \}.$$

Remark, that for any $i \in \mathbb{Z}/h\mathbb{Z}$ $\mathcal{H}_i$ is completely determined by its projection $\mathcal{H}_i(\chi)$ to $\mathrm{Hom}_{W(\bar{\mathbb{F}}_p)}(U_\chi, U_{\sigma^i\chi})$. If $i \neq 0$, then $\mathcal{H}_i(\chi) = p^{n(i)}W(\mathbb{F}_q)e_{0,i}$.

If $i \in \mathbb{Z}/h\mathbb{Z} \setminus \{0\}$, then one can easily verify, that $[\mathcal{H}_i, \mathcal{H}_{-i}] \subset \mathcal{H}_0$ consists of elements in a form

$$p^{n(i)+n(-i)} \sum_{m\in\mathbb{Z}/h\mathbb{Z}} \alpha_m e_{m,m},$$

where $\alpha_0 = \sigma^i\gamma - \gamma$ for some $\gamma \in W(\mathbb{F}_q)$.

If $h_1|h$, denote by Tr_{h,h_1} the trace map of the fields extension given by quotient fields of the rings $W(\mathbb{F}_q) = W(\mathbb{F}_{p^h})$ and $W(\mathbb{F}_{p^{h_1}})$. One can easily check up the following statement

Lemma. *If $\alpha \in W(\mathbb{F}_q), i \in \mathbb{Z}/h\mathbb{Z}$, then the following conditions are equivalent*

1) *there exists $\gamma \in W(\mathbb{F}_q)$, such that $\alpha = \sigma^i\gamma - \gamma$;*

2) *if $h_1 = c.g.d.(h, i)$, then $\mathrm{Tr}_{h,h_1} \alpha = 0$.*

Therefore, if $i \in \mathbb{Z}/h\mathbb{Z} \setminus \{0\}$, then the property $[\mathcal{H}_i, \mathcal{H}_{-i}] \subset \mathcal{H}_0$ is equivalent to

$$p^{n(i)+n(-i)} \mathrm{Ker}(\mathrm{Tr}_{h,(h,i)})e_{0,0} \subset \mathcal{H}_0(\chi).$$

Definition.

a) If $h_1|h$, then

$$n^*(h_1) = \min\{ n(i) + n(-i) \mid i \in \mathbb{Z}/h\mathbb{Z} \setminus \{0\}, (i,h) = h_1 \};$$

b) $W^{(n)} = \sum_{h_1|h} p^{n^*(h_1)} \mathrm{Ker}\,\mathrm{Tr}_{h,h_1} \subset W(\mathbb{F}_q)$.

Clearly, $W^{(n)}$ is the minimal $\mathbb{Z}_p$-submodule in $W(\mathbb{F}_p)$ containing $\mathbb{Z}_p$-modules $p^{n(i)+n(-i)}\mathrm{Ker}\,\mathrm{Tr}_{h,(h,i)}$ for all $i \in \mathbb{Z}/h\mathbb{Z} \setminus \{0\}$.

Finally, we obtain

Proposition. *There is a one-to-one correspondence between pairs (H, χ), where H is a subgroup of $\mathrm{Aut}_{\mathbb{Z}_p} U$, which satisfies properties C1, C3, C4, and χ is a fixed character of the H-module $U \otimes \mathbb{F}_p$, and the following data:*

1) *a function $n = n_{H,\chi} : \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}$, such that*

$$n(0) = \min\{ n(i) + n(-i) \mid i \in \mathbb{Z}/N\mathbb{Z} \}$$

and

$$n(i) + n(j) \geq n(i+j)$$

for all $i, j \in \mathbb{Z}/h\mathbb{Z}$;

2) *a* $\mathbb{Z}_p$*-module* $\mathcal{H}_0(\chi) = \mathcal{H}_0(H, \chi)$, *such that*

$$W^{(n)} e_{0,0} \subset \mathcal{H}_0(\chi) \subset pW(\mathbb{F}_q) e_{0,0}.$$

2. Case of Fontaine-Laffaille modules.

Let $W(k)$ be the ring of Witt vectors with coefficients in a perfect field k of characteristic $p > 0$. Let K be its quotient field and $\Gamma = \mathrm{Gal}(\bar{K}/K)$. Let U be a free $\mathbb{Z}_p$-module of finite rank h with continuos Γ-action. If the image H of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} U$ satisfies the properties C1-C3, we also use notation $n_U, n_{U,\chi}$ instead of $n_H, n_{H,\chi}$ from section 1. Under above assumptions C1-C3 we want to study the case, when U is Fontaine-Laffaille Γ-module, i.e. U is a Γ-invariant lattice in some crystalline $\mathbb{Q}_p[\Gamma]$-module with Hodge-Tate weights from $[0, a]$, where $a < p$. For simplicity we assume, that k is algebraically closed (what is equivalent to the study of the image of the inertia subgroup of Γ).

2.1. *Some facts from Fontaine-Laffaille theory,* [F-L].

Let A_{cris} be Fontaine's crystalline ring. It has continuos Γ-action, $A_{\mathrm{cris}}^{\Gamma} = W(k)$. There is Frobenius endomorphism $\sigma_{\mathrm{cris}}(= \sigma)$ of A_{cris}, which prolongs standard Frobenius σ of $W(k)$. A_{cris} has a decreasing filtration of ideals $\mathrm{Fil}^i A_{\mathrm{cris}}$, such that $\sigma \,\mathrm{Fil}^i A_{\mathrm{cris}} \subset p^i A_{\mathrm{cris}}$ for $0 \leq i < p$.

Let $\mathcal{MF}$ be the category of $W(k)$-modules M with decreasing filtration of length $< p$ by $W(k)$-submodules $M = M^0 \supset M^1 \supset \cdots \supset M^p = 0$ and σ-linear morphisms $\phi_i : M^i \longrightarrow M$, such that $\phi_i|_{M^{i+1}} = p\phi_{i+1}$ for all $0 \leq i < p$.

One can consider A_{cris} as the object of the category $\mathcal{MF}$, if $A_{\mathrm{cris}}^i = \mathrm{Fil}^i A_{\mathrm{cris}}$, $\phi_i = p^{-i}\sigma$ for $0 \leq i < p$, and $A_{\mathrm{cris}}^p = 0$.

Let MF be the full subcategory of admissible modules in $\mathcal{MF}$. By definition, MF consists of finitely generated filtered modules $M \in \mathcal{MF}$, such that $\sum_i \phi_i(M^i) = M$. MF is an abelian category. Denote by MF_f (resp., $\mathrm{MF}_{\mathrm{tor}}$) a full subcategory of MF which consists of free (resp., torsion) $W(k)$-modules M.

Let $\mathrm{M}\Gamma$ be the category of $\mathbb{Z}_p[\Gamma]$-modules. Then Fontaine-Laffaille theory gives an exact and faithfull functor $\mathcal{U} : \mathrm{MF} \longrightarrow \mathrm{M}\Gamma$. If $M \in \mathrm{MF}_f$, then $\mathcal{U}(M) = \mathrm{Hom}_{\mathcal{MF}}(M, A_{\mathrm{cris}})$, where the structure of Γ-module on $\mathcal{U}(M)$ is induced from the Γ-module structure on A_{cris}. In this case $\mathcal{U}(M)$ is a free $\mathbb{Z}_p$-module, $\mathrm{rk}_{\mathbb{Z}_p} \mathcal{U}(M) = \mathrm{rk}_{W(k)} M$ and $\mathcal{U}(M) \otimes \mathbb{Q}_p$ is a crystalline $\mathbb{Q}_p[\Gamma]$-module with weights from $[a, b]$, if $M^0 = M^a$ and $M^{b+1} = 0$. If $M \in \mathrm{MF}_{\mathrm{tor}}$, then $\mathcal{U}(M) = \mathrm{Hom}_{\mathcal{MF}}(M, A_{\mathrm{cris},\infty})$, where $A_{\mathrm{cris},\infty} = \varinjlim_{n \in \mathbb{N}} A_{\mathrm{cris},n}$, and $A_{\mathrm{cris},n} = A_{\mathrm{cris}}/p^n A_{\mathrm{cris}}$ with induced structure of the object of the category $\mathcal{MF}$. In this case lengths of $W(k)$-module M and of $\mathbb{Z}_p$-module $\mathcal{U}(M)$ coincide.

First information about Γ-modules $\mathcal{U}(M)$, where $M \in \mathrm{MF}$, comes from the study of simple objects of the category MF. Let $R_p = \{ r \in \mathbb{Q} \cap [0,1] \mid v_p(r) \geq 0 \}$. For any $r \in R_p$ consider its archimedian decomposition

$$r = \frac{l_0(r)}{p} + \cdots + \frac{l_s(r)}{p^{s+1}} + \ldots$$

with digits $l_s(r)$, where $0 \le l_s(r) < p$ for all $s \in \mathbb{Z}_{\ge 0}$. Denote by $h(r)$ the minimal period of the sequence $\{l_s(r)\}_{s\ge 0}$. One can use indices from $\mathbb{Z}/h(r)\mathbb{Z}$ or from $\mathbb{Z}$ for this sequence.

Let $r \in R_p$ and $M(r) \in \mathrm{MF}$ be such that

a) $pM(r) = 0$ and as k-module $M(r)$ has a basis $\{m_i \mid i \in \mathbb{Z}/h(r)\mathbb{Z}\}$;

b) for $0 \le j < p$ the submodule of filtration $M(r)^j$ is generated by

$$\{m_i \mid l_i(r) \ge j, i \in \mathbb{Z}/h(r)\mathbb{Z}\ \}$$

(in particular, $m_i \in M(r)^{l_i(r)} \setminus M(r)^{l_i(r)+1}$);

c) for all $i \in \mathbb{Z}/h(r)\mathbb{Z}$ one has $\phi_{l_i(r)}(m_i) = m_{i+1}$.

If $r \in R_p$ and $i \in \mathbb{Z}$, let

$$r(i) = \frac{l_i(r)}{p} + \cdots + \frac{l_{i+s}(r)}{p^{s+1}} + \ldots .$$

Then any simple object of the category MF is isomorphic to $M(r)$ for some $r \in R_p$, and $M(r_1) \simeq M(r)$ iff $r_1 = r(i)$ for some $i \in \mathbb{Z}$.

If $N \in \mathbb{N}$ introduce "tamely ramified" character $\chi_N^* : \Gamma \longrightarrow W(k)^*$ by the relation

$$\chi_N^*(\tau) = (\tau\pi_N)/\pi_N,$$

where $\tau \in \Gamma$ and $\pi_N \in \bar{K}$ is such that $\pi_N^{p^N-1} = -p$. If $\chi : \Gamma \longrightarrow W(k)^*$ is some continuos character, then $\chi = \chi_N^{*k_N(\chi)}$ for some $N \in \mathbb{N}$ and $0 \le k_N(\chi) < p^N - 1$. In this notation

$$r(\chi) = k_N(\chi)/(p^N - 1) \in R_p \cap [0, 1)$$

does not depend on the choice of N and determines the character χ uniquelly. One can use this invariant to describe the structure of Γ-module $U(r) = \mathcal{U}(M(r))$. If $r \in R_p \cap [0, 1)$, then $U(r)$ is a simple $\mathbb{Z}_p[\Gamma]$-module with the set of characters $S = \{\chi, \sigma\chi, \ldots, \sigma^{h(r)-1}\chi\}$, where $r(\chi) = r$. This means $pU(r) = 0$ and

$$U(r) \otimes W(k) = \oplus_{\eta \in S} U(r)_\eta,$$

where $U(r)_\eta = \{u \in U(r) \otimes W(k) \mid \tau u = \eta(\tau)u \ \text{ for all } \tau \in \Gamma\} \ne 0$. If $r = 1$, then $U(1) = U(0)$ is trivial Γ-module $\mathbb{F}_p$.

Let V be a crystalline $\mathbb{Q}_p[\Gamma]$-module with weights from $[0, p-1]$. We call Γ-module U Fontaine-Laffaille Γ-module, if U is isomorphic to some Γ-invariant $\mathbb{Z}_p$-lattice of V. By the main result of Fontaine-Laffaille theory V contains some Γ-invariant lattice isomorphic to $\mathcal{U}(M)$ for some $M \in \mathrm{MF}_f$. Generally, one can not present any Γ-invariant lattice of V as $\mathcal{U}(M)$, where $M \in \mathrm{MF}_f$, because the functor $\mathcal{U} : \mathrm{MF} \longrightarrow \mathrm{M}\Gamma$ is not fully faithfull. Let MF^u be a full subcategory of MF, which consists of filtered modules $M \in \mathrm{MF}$, such that the simple object $M(1)$ does not appear as a subquotient of M. Then restriction

$$\mathcal{U} : \mathrm{MF}^u \longrightarrow \mathrm{M}\Gamma$$

is fully faithfull functor. So, if $U_1 \subset \mathcal{U}(M) \otimes \mathbb{Q}_p$, where $M \in \mathrm{MF}_f^u$, is Γ-invariant lattice, then $U_1 = \mathcal{U}(M_1)$ for some $M_1 \in \mathrm{MF}_f^u$. In this case

$$M_1 = \mathrm{Hom}^{\Gamma}(U_1, A_{\mathrm{cris}}),$$

where the filtration and σ-linear morphisms ϕ_i, $0 \le i < p$, on M_1 are induced from those on A_{cris}. (One can apply modification of the Fontaine-Laffaille functor from [Ab1] to describe all Γ-invariant lattices of arbitrary crystalline $\mathbb{Q}_p[\Gamma]$-module with weights from $[0, p-1]$.)

At least in our case, properties of the Γ-module $U = \mathcal{U}(M)$ are related more directly to properties of the filtered module $M' \in \mathrm{MF}^u$, such that $U = \mathcal{U}_1(M')$, where $\mathcal{U}_1 : \mathrm{MF}^u \longrightarrow \mathrm{M}\Gamma$ is some functor equivalent to the functor $\mathcal{U}$. Let MF_1^u be a full subcategory of MF^u, which consists of filtered modules M, such that $pM = 0$. Then construction of $\mathcal{U}_1|_{\mathrm{MF}_1^u}$ was done in [Ab1] (where the more general case of objects $M \in \mathrm{MF}$, such that $pM = 0$, was considered). Essential part of this construction can be explained as follows.

Let $M \in \mathrm{MF}_1^u$, then it has k-basis $\bar{m} = (m_1, \dots, m_N)$, such that for some function $l : [1, N] \longrightarrow [0, p-1]$ the filtration submodule $M^j, 0 \le j < p$, is generated by $\{ m_i \mid l(i) \ge j \}$. If $\bar{\phi}(\bar{m}) = (\phi_{l(1)}(m_1), \dots, \phi_{l(N)}(m_N))$, then σ-linear morphisms ϕ_k, $0 \le k < p$, are uniquelly defined by the relation

$$\bar{\phi}(\bar{m}) = \bar{m}C,$$

for some $C \in \mathrm{GL}_N(W(k))$. Then $\mathcal{U}_1(M)$ can be identified with Γ-module of residues modulo $p\bar{O}$ of $\bar{K}$-solutions $\bar{X} = (X_1, \dots, X_N)$ of the system of equations

$$\left(\frac{X_1^p}{(-p)^{l(1)}}, \dots, \frac{X_N^p}{(-p)^{l(N)}} \right) = (X_1, \dots, X_N)C.$$

Construction of equivalence of the functors $\mathcal{U}|_{\mathrm{MF}_1^u}$ and $\mathcal{U}_1|_{\mathrm{MF}_1^u}$ is relatively complicated, c.f. [Ab1] (and leads to the construction of the functor $\mathcal{U}_1$). But, if $\mathrm{MF}(p-2)$ is a full subcategory of MF, which consists of filtered modules M, such that $M^{p-1} = 0$, then restrictions of $\mathcal{U}$ and $\mathcal{U}_1$ on $\mathrm{MF}(p-2)$ coincide. So, we can considerably simplify out arguments by studying only the case of Fontaine-Laffaille modules in a form $\mathcal{U}(M)$, where $M \in \mathrm{MF}(p-2)$. Remark, that objects M of the category $\mathrm{MF}(p-2)$ are characterized by the following property:

if $M(r)$ is a simple subquotent of M, then $r \in R_p(p-2)$, where

$$R_p(p-2) = \{ r \in R_p \mid 0 \le l_s(r) \le p-2 \ \text{ for all } s \ge 0 \}.$$

2.2. *Class* $\mathrm{MF}^{(S)}$.

Let S be a finite subset of R_p, such that $r \in S \Rightarrow r(1) \in S$. For any $r \in S$ we denote its archimedean decomposition in "a base p" by

$$r = \frac{l_0(r)}{p} + \dots + \frac{l_s(r)}{p^{s+1}} + \dots,$$

where $0 \le l_s(r) < p$ for all $s \in \mathbb{Z}_{\ge 0}$.

Introduce class $\mathrm{MF}^{(S)}$ of objects of the category MF_f as follows. By definition it consists of filtered free $W(k)$-modules M, such that

a) M has $W(k)$-basis $\{m_r \mid r \in S\}$ and for any $0 \le j \le p$ its filtration submodule M^j is generated by $\{m_r \mid l_0(r) \ge j\}$ (in particular, for any $r \in S$ one has $m_r \in M^{l_0(r)} \setminus M^{l_0(r)+1}$);

b) σ-linear morphisms $\phi_j : M^j \longrightarrow M$ are uniquelly defined by relations

$$\phi_{l_0(r(-1))} m_{r(-1)} = m_r + \sum_{r' \in S} \beta_{rr'} m_{r'}$$

where $r \in S$ and coefficients $\beta_{rr'} \in W(k)$ satisfy the following conditions b_1) and b_2).

b_1) Let $r_1, \dots, r_m \in S$ be such that

$$S = \{r_1, \dots, r_1(h_1 - 1); \dots ; r_m, \dots, r_m(h_m - 1)\},$$

where $h_j = h(r_j)$ is the minimal period of p-digits decomposition for $r_j \in S$. There exists substitution $\begin{pmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{pmatrix}$, such that

if $r = r_{j_a}(\alpha), r' = r_{j_b}(\beta)$, *where* $a \ge b$, $\alpha \in \mathbb{Z}/h_{j_a}\mathbb{Z}, \beta \in \mathbb{Z}h_{j_b}\mathbb{Z}$, *then* $\beta_{rr'} \in pW(k)$;

b_2) *if* $l_0(r) \le l_0(r')$, *then* $\beta_{rr'} = 0$.

The above conditions a) and b_1) define on M the structure of an object of the category MF_f and the condition b_1) describes $M/pM = M^{(1)} \in \mathrm{MF}_{\mathrm{tor}}$ as subsequent extensions of the simple object $M(r_{j_1})$ by $M(r_{j_a})$, where $1 < a \le m$. In other words, one has the following exact sequences in the category $\mathrm{MF}_{\mathrm{tor}}$:

$$0 \longrightarrow M^{(2)} \longrightarrow M^{(1)} \longrightarrow M(r_{j_1}) \longrightarrow 0$$

....

$$0 \longrightarrow M(r_{j_m}) = M^{(m)} \longrightarrow M^{(m-1)} \longrightarrow M(r_{j_{m-1}}) \longrightarrow 0.$$

The condition b_2) was introduced by Wintenberger, c.f. [Wtb]. He proved, that the structure of any $M \in \mathrm{MF}_f$ has the above explicit description, which satisfies this additional property (and even gives a functorial spritting of the filtration on M).

If U is a free $\mathbb{Z}_p$-module with continuos action of Γ, and $H = H(U)$ is the image of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} U$, then $\mathbb{Z}_p[H]$-module U automatically satisfies the property C1 of n.1. In notation of n.1 H^1 is the image of the higher ramification subgroup I of Γ and H_1 is identified with a quotient of $\Gamma_{\mathrm{tr}} = \Gamma/I$. We can fix a section $s : \Gamma_{\mathrm{tr}} \longrightarrow \Gamma$ of the projection $\Gamma \longrightarrow \Gamma_{\mathrm{tr}}$ and take induced splitting $s : H_1 \longrightarrow H$. Therefore, any character χ of $s(H_1)$ can be considered as character of Γ_{tr} (this identification is induced by composition $\Gamma_{\mathrm{tr}} \xrightarrow{s} s(\Gamma_{\mathrm{tr}}) \longrightarrow s(H_1)$) and can be given by its r-invariant $r(\chi)$ from n.2.1.

Clearly, $\mathrm{MF}^{(S)} \subset \mathrm{MF}(p-2)$, if and only if $S \subset R_p(p-2)$. If $M \in \mathrm{MF}^{(S)}$ and $U = \mathcal{U}(M)$, then the set $S(H)$ of characters of the group $s(H_1)$, which appears in n.1, is identified with S by the correspondence $\chi \mapsto r(\chi)$. So, U satisfies the property C2 of n.1. We obtained the following proposition.

Proposition. *The following statements are equivalent:*

1) *U is Fontaine-Laffaille module with weights from $[0, p-2]$, which satisfies conditions* C1 *and* C2 *of n.1;*

2) *$U \simeq \mathcal{U}(M)$, where $M \in \mathrm{MF}^{(S)}$ and $S = S(H(U)) \subset R_p(p-2)$.*

Consider the following property of $S \subset R_p(p-2)$.

C5. *All elements of the set*

$$\{\ (r_1 - r_2) \bmod \mathbb{Z} \mid r_1, r_2 \in S, r_1 \neq r_2\ \}$$

are different.

Then we have

Corollary. *U is Fontaine-Laffaille Γ-module with weights from $[0, p-2]$ satisfying conditions* C1-C3 *of n.1, if and only if $U \simeq \mathcal{U}(M)$, where $M \in \mathrm{MF}^{(S)}$ and $S \subset R_p(p-2)$ satisfies the above property* C5.

2.3. *Function n_M.*

Let $M \in \mathrm{MF}^{(S)}$ be given in notation of n.2.2.

Define the function $n_M : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ as follows.

For $r, r' \in S$ set

$$n_M^*(r, r') = \min\{\ v_p(\beta_{r'(i), r(i)}) \mid i \in \mathbb{Z}\},$$

then for $r_1, r_2 \in S$

$$n_M(r_1, r_2) =$$

$$= \min\{\ n_M^*(r_1, r^{(1)}) + \cdots + n_M^*(r^{(l-1)}, r^{(l)}) + n_M^*(r^{(l)}, r_2) \mid l \geq 0, r^{(1)}, \ldots, r^{(l)} \in S\ \}.$$

Proposition. *The function n_M satisfies the following properties:*

1) *$n_M(r, r) \geq 1$ for any $r \in S$;*

2) *$n_M(r_1(1), r_2(1)) = n_M(r_1, r_2)$ for any $r_1, r_2 \in S$;*

3) *for any $r_1, r_2, r_3 \in S$*

$$n_M(r_1, r_2) \leq n_M(r_1, r_3) + n_M(r_3, r_2);$$

4) *if $r_1, r_2 \in S$ and for all $i \in \mathbb{Z}$ holds $l_0(r_1(i)) \geq l_0(r_2(i))$, then*

$$n_M(r_1, r_2) = \min\{n_M(r_1, r) + n_M(r, r_2) \mid r \in S\}.$$

Proof. 1) follows from the property b_1) of coefficients $\beta_{rr'}$;

2) follows from the equality $n_M^*(r(1), r'(1)) = n_M^*(r, r')$;

3) follows from definition of $n_M(r_1, r_2)$.

4) If $n_M(r_1, r_2) = +\infty$, then this equality follows from the above n.3). If $n_M(r_1, r_2) < +\infty$, then

$$n_M(r_1, r_2) = n_M^*(r_1, r^{(1)}) + \cdots + n_M^*(r^{(l)}, r_2),$$

for some $l \geq 1$ and $r^{(1)}, \dots, r^{(l)} \in S$, because $n_M^*(r_1, r_2) = +\infty$ by the property b_2) of n.2.2. Then by definition of n_M we have

$$n_M^*(r_1, r^{(1)}) \geq n_M(r_1, r^{(1)}), \quad n_M^*(r^{(1)}, r^{(2)}) + \dots + n_M^*(r^{(l)}, r_2) \geq n_M(r^{(1)}, r_2).$$

This gives

$$n_M(r_1, r_2) \geq n_M(r_1, r^{(1)}) + n_M(r^{(1)}, r_2).$$

Now it is sufficient to remark, that by the above property 3)

$$n_M(r_1, r_2) \leq \min\{n_M(r_1, r_3) + n_M(r_3, r_2) \mid r_3 \in S\}.$$

Remark.

It is not clear from the above definition of the function n_M, that it depends only on the isomorphism class of $M \in \mathrm{MF}^{(S)}$ in the category MF. This property can be proved from functoriality of Wintenberger splitting, c.f. [Wtb]. This follows also from theorem A of n.2.5.1 below.

2.4. *Semilinear functions and their graphs.*

2.4.1. Let S be a finite set. Denote by $\mathcal{F}_S$ the set of functions

$$n : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\},$$

such that for all $r_1, r_2, r_3 \in S$ one has

$(1_\mathcal{F})$ $n(r_1, r_1) \geq 1$;

$(2_\mathcal{F})$ $n(r_1, r_2) \leq n(r_1, r_3) + n(r_3, r_2)$.

If $S_1 \subset S \times S$ and $(r_1, r_2) \in S_1$, denote by $S_1(r_1, r_2)$ the set of sequences $(r_1, r^{(1)}, \dots, r^{(l)}, r_2)$, where $l \geq 0$ and $(r_1, r^{(1)}), \dots, (r^{(l)}, r_2) \in S_1$ (in the oriented graph with vertices S and edges S_1 this set is the set of all paths, which connect r_1 and r_2).

Denote by $\mathcal{V}_S$ the set of functions

$$v : S_v \longrightarrow \mathbb{Z}_{\geq 0},$$

where $S_v \subset S \times S$ and

$(1_\mathcal{V})$ *if* $(r_1, \dots, r^{(l)}, r) \in S_v(r, r)$, *then*

$$v(r, r^{(1)}) + \dots + v(r^{(l)}, r) \geq 1;$$

$(2_\mathcal{V})$ *if* $(r_1, r_2) \in S_v$ *and* $(r_1, \dots, r^{(l)}, r_2) \in S_v(r_1, r_2)$, *where* $l \geq 1$, *then*

$$v(r_1, r_2) < v(r_1, r^{(1)}) + \dots + v(r^{(l)}, r_2).$$

So, $\mathcal{V}_S$ is the set of oriented graphs with nonnegative integral metrics, where edges are shortest paths between their vertices and there are no cycles of length 0.

If $n \in S$, let

$$S^{(n)} = \{(r_1, r_2) \in S \times S \mid n(r_1, r_2) < n(r_1, r_3) + n(r_3, r_2) \ \forall r_3 \in S \ \}$$

and consider the function $\pi(n) : S^{(n)} \longrightarrow \mathbb{Z}_{\geq 0}$, such that $\pi(n)(r_1, r_2) = n(r_1, r_2)$ (if $(r_1, r_2) \in S^{(n)}$).

We have: $\pi(n) \in \mathcal{V}_S$.

Indeed, $(1_{\mathcal{F}})$ and $(2_{\mathcal{F}})$ imply $(1_{\mathcal{V}})$. If $(2_{\mathcal{V}})$ does not hold, then there exists $(r_1, r^{(1)}, \ldots, r^{(l)}, r_2) \in S^{(n)}(r_1, r_2)$, where $l \geq 1$, such that

$$\pi(n)(r_1, r_2) \geq \pi(n)(r_1, r^{(1)}) + \cdots + \pi(n)(r^{(l)}, r_2).$$

This gives $n(r_1, r_2) \geq n(r_1, r^{(1)}) + n(r^{(1)}, r_2)$ and we obtain contradiction $(r_1, r_2) \notin S^{(n)}$.

So, we defined the map $\pi : \mathcal{F}_S \longrightarrow \mathcal{V}_S$.

Let $v \in \mathcal{V}_S$. If $S_v(r_1, r_2) = \emptyset$, set $\eta(v)(r_1, r_2) = +\infty$. Otherwise, let

$$\eta(v)(r_1, r_2) = \min\{v(r_1, r^{(1)}) + \cdots + v(r^{(l)}, r_2) \mid (r_1, \ldots, r^{(l)}, r_2) \in S_v(r_1, r_2) \ \}.$$

Clearly, $\eta(v) \in \mathcal{F}_S$ and we defined the map $\eta : \mathcal{V}_S \longrightarrow \mathcal{F}_S$.

2.4.2. Proposition. *π and η are inverse one to another bijections of the sets $\mathcal{F}_S$ and $\mathcal{V}_S$.*

Proof.

1) Prove, that $\pi\eta = \mathrm{id}_{\mathcal{F}_S}$.

Let $n \in \mathcal{F}_S$, $v = \pi(n) \in \mathcal{V}_S$. We want to prove, that for any $(r_1, r_2) \in S \times S$

$$\eta(v)(r_1, r_2) = n(r_1, r_2).$$

This is implied by the following lemma.

Lemma.

a) *If $\eta(v)(r_1, r_2) < +\infty$, then $n(r_1, r_2) \leq \eta(v)(r_1, r_2)$.*

b) *If $n(r_1, r_2) < +\infty$, then $\eta(v)(r_1, r_2) \leq n(r_1, r_2)$.*

Proof of lemma.

a) $\eta(v)(r_1, r_2) < +\infty \Rightarrow S^{(n)}(r_1, r_2) \neq \emptyset \Rightarrow$

$$\eta(v)(r_1, r_2) = \min\{v(r_1, r^{(1)}) + \cdots + v(r^{(l)}, r_2) \mid (r_1, \ldots, r^{(l)}, r_2) \in S^{(n)}(r_1, r_2) \ \}.$$

From definition of $v = \pi(n)$ it follows, that $v(r_1, r^{(1)}) = n(r_1, r^{(1)}), \ldots, v(r^{(l)}, r_2) = n(r^{(l)}, r_2)$ and, therefore, $\eta(v)(r_1, r_2) \geq n(r_1, r_2)$.

b) Let $n(r_1, r_2) < +\infty$. Then one can find a presentation

$$(*) \qquad n(r_1, r_2) = n(r_1, r^{(1)}) + \cdots + n(r^{(l)}, r_2),$$

where $r^{(1)}, \ldots, r^{(l)} \in S$ and the number of summands $l + 1 = l(r_1, r_2)$ is maximal.

Indeed, the set of such presentations is not empty (one can take $l = 0$). But the number of summands of these presentations is certainly restricted, because for any $r_0, \ldots, r_{|S|} \in S$ we have the inequality

$$n(r_0, r_1) + \cdots + n(r_{|S|-1}, r_{|S|}) \geq 1$$

(there exist $0 \leq i < j \leq |S|$, such that $r_i = r_j$, then the left-hand side is not less, than $n(r_i, r_{i+1}) + \cdots + n(r_{j-1}, r_j) \geq n(r_i, r_j) \geq 1$).

From the above maximal property of the presentation $(*)$ it follows now, that $(r_1, r^{(1)}), \ldots, (r^{(l)}, r_2) \in S^{(n)}$, therefore, $S^{(n)}(r_1, r_2) \neq \emptyset$, and $\eta(v)(r_1, r_2) \leq n(r_1, r_2)$.

Lemma is proved.

2) Prove, that $\eta\pi = \mathrm{id}_{\mathcal{V}_S}$.

Let $v \in \mathcal{V}_S$ and $n = \eta(v) \in \mathcal{F}_S$.

From definitions of elements of the set $\mathcal{V}_S$ and of the map η it follows, that one has $n(r_1, r_2) = v(r_1, r_2)$, if $(r_1, r_2) \in S_v$. So,

$$\pi(n) = v \ \Leftrightarrow \ \ S_v = S^{(n)}.$$

Prove, that $S_v \subset S^{(n)}$.

Take $(r_1, r_2) \in S_v$ and some $r_3 \in S$. If either $S_v(r_1, r_3) = \emptyset$ or $S_v(r_3, r_2) = \emptyset$, then $n(r_1, r_2) < +\infty = n(r_1, r_3) + n(r_3, r_2)$.

If $S_v(r_1, r_3) \neq \emptyset$ and $S_v(r_3, r_2) \neq \emptyset$, then

$$n(r_1, r_3) = v(r_1, r'^{(1)}) + \cdots + v(r'^{(l_1)}, r_3)$$

and

$$n(r_3, r_2) = v(r_3, r''^{(1)}) + \cdots + v(r''^{(l_2)}, r_2)$$

for some $(r_1, r'^{(1)}, \ldots, r'^{(l_1)}, r_3) \in S_v(r_1, r_3)$, $(r_3, r''^{(1)}, \ldots, r''^{(l_2)}, r_2) \in S_v(r_3, r_2)$. Now by the property $(2_{\mathcal{V}})$ we have here also $n(r_1, r_2) < n(r_1, r_3) + n(r_3, r_2)$.

So, $n(r_1, r_2) < n(r_1, r_3) + n(r_3, r_2)$ for all $r_3 \in S$, i.e. $(r_1, r_2) \in S^{(n)}$.

Prove, that $S^{(n)} \subset S_v$.

Let $(r_1, r_2) \in S^{(n)}$, then $n(r_1, r_2) < +\infty$, $S_v(r_1, r_2) \neq \emptyset$ and $n(r_1, r_2) = n(r_1, r^{(1)}) + \cdots + n(r^{(l)}, r_2)$ for some $(r_1, r^{(1)}, \ldots, r^{(l)}, r_2) \in S_v(r_1, r_2)$. If $l \geq 1$, let $r_3 = r^{(1)}$. Then $n(r^{(1)}, r^{(2)}) + \cdots + n(r^{(l)}, r_2) \geq n(r_3, r_2)$, and $n(r_1, r_2) \geq n(r_1, r_3) + n(r_3, r_2)$. This gives contradiction $(r_1, r_2) \notin S^{(n)}$. Therefore, $l = 0$ and $(r_1, r_2) \in S_v$.

Proposition is proved.

2.4.3. We use the following criterium in n.3 below.

Proposition. *Let $n_1, n_2 \in \mathcal{F}_S$ be such that*

1) $n_1(r_1, r_2) \geq n_2(r_1, r_2)$ *for any* $r_1, r_2 \in S$;

2) *if* $\pi(n_2) = v_2 \in \mathcal{V}_S$ *and* $(r_1, r_2) \in S_{v_2}$, *then* $n_1(r_1, r_2) \leq v_2(r_1, r_2)$.

Then $n_1 = n_2$.

Proof. Let $v_1 = \pi(n_1) \in \mathcal{V}_S$. Then

$$S_{v_1} \supset S_{v_2}.$$

Indeed, $(r_1, r_2) \in S_{v_2} \ \Rightarrow$

$$\Rightarrow n_1(r_1,r_2) \le v_2(r_1,r_2) = n_2(r_1,r_2) < n_2(r_1,r_3)+n_2(r_3,r_2) \le n_1(r_1,r_3)+n_1(r_3,r_2)$$

for all $r_3 \in S$, i.e. $(r_1, r_2) \in S_{v_1}$.

Clearly, $v_1|_{S_{v_2}} \le v_2$.

Now, for any $(r_1, r_2) \in S \times S$ we have

$$S_{v_2}(r_1, r_2) \subset S_{v_1}(r_1, r_2)$$

and, therefore, $n_1(r_1, r_2) = \eta(v_1)(r_1, r_2) =$

$$= \min\{ \ v_1(r_1, r^{(1)}) + \cdots + v_1(r^{(l)}, r_2) \mid (r_1, \ldots, r^{(l)}, r_2) \in S_{v_1}(r_1, r_2) \ \} \le$$

$$\min\{ \ v_2(r_1, r^{(1)}) + \cdots + v_2(r^{(l)}, r_2) \mid (r_1, \ldots, r^{(l)}, r_2) \in S_{v_2}(r_1, r_2) \ \} = n_2(r_1, r_2).$$

Proposition is proved.

2.4.4. Let S be a finite subset in R_p, such that $r \in S \Rightarrow r(1) \in S$.

Let $n \in \mathcal{F}_S$ and $\pi(n) = v \in \mathcal{V}_S$. The above description of the correspondence $n \leftrightarrow v$ implies the following proposition.

Proposition. *The following statements* 1) *and* 2) *are equivalent:*

1) a) *for any* $r_1, r_2 \in S$ *one has* $n(r_1(1), r_2(1)) = n(r_1, r_2)$*;*

b) *if* $r_1, r_2 \in S$ *and* $l_0(r_1(i)) \ge l_0(r_2(i))$ *for all* $i \in \mathbb{Z}$*, then*

$$n(r_1, r_2) = \min\{n(r_1, r_3) + n(r_3, r_2) \mid r_3 \in S\}$$

2) a) *if* $(r_1, r_2) \in S_v$*, then there exists* $i \in \mathbb{Z}$*, such that*

$$l_0(r_1(i)) < l_0(r_2(i))$$

(in particular, $(r, r) \notin S_v$ *for any* $r \in S$*);*

b) *if* $(r_1, r_2) \in S_v$*, then* $(r_1(1), r_2(1)) \in S_v$ *and*

$$v(r_1, r_2) = v(r_1(1), r_2(1)).$$

2.5. *Main statements.*

Let $S \subset R_p(p-2)$ be a finite set, such that $r \in S \Rightarrow r(1) \in S$, and S satisfies the condition C5 of n.2.3.

2.5.1. Let $M \in \mathrm{MF}^{(S)}$ and $U = \mathcal{U}(M)$. If $H(M)$ is the image of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} \mathcal{U}(M)$, then $S = S(H(M))$ and by proposition of n.1.2 we have the function

$$n_{H(M)} = n_{\mathcal{U}(M)} : S \times S \longrightarrow \mathbb{Z}_{\ge 0} \cup \{+\infty\}$$

(we use identification of characters of $s(H_1)$ with elements of S, c.f. n.2.2).

Let

$$n_M : S \times S \longrightarrow \mathbb{Z}_{\ge 0} \cup \{+\infty\}$$

be the function defined in n.2.2.3.

Theorem A. *In the above notation* $n_{\mathcal{U}(M)} = n_M$.

We prove this theorem in n.3 below.

2.5.2. Let a function

$$n : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$$

be such that for any $r_1, r_2, r_3 \in S$

a) $n(r_1, r_1) \geq 1$;

b) $n(r_1, r_2) = n(r_1(1), r_2(1))$;

c) $n(r_1, r_2) \leq n(r_1, r_3) + n(r_3, r_2)$;

d) $n(r_1, r_1) = \min\{\ n(r_1, r) + n(r, r_1) \mid r \in S\ \}$.

From n.1 it follows, that this function n can be related to some subgroup $H \subset \mathrm{Aut}_{\mathbb{Z}_p} U$, where U is a free $\mathbb{Z}_p$-module, $\mathrm{rk}_{\mathbb{Z}_p} U = |S|$. The above aggreement about identification of characters of $s(H_1)$ with characters of Γ_{tr} gives epimorphism $\Gamma_{\mathrm{tr}} \longrightarrow H_1$. One can check up, that this epimorphism can be prolonged to some epimorphism $\Gamma \longrightarrow H$. Therefore, any such function n arises from some $\mathbb{Z}_p[\Gamma]$-module U.

If $U = \mathcal{U}(M)$, where $M \in \mathrm{MF}^{(S)}$, then proposition of n.2.3 and the above theorem A imply, that the function $n = n_{\mathcal{U}(M)}$ satisfies the following property d'), which is stronger, than the property d).

d') if $r_1, r_2 \in S$ and $l_0(r_1(i)) \geq l_0(r_2(i))$ for all $i \in \mathbb{Z}$, then

$$n(r_1, r_2) = \min\{\ n(r_1, r) + n(r, r_2) \mid r \in S\ \}.$$

Theorem B. *If* $n : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ *satisfies the above properties a)-c) and d'), then there exists $M \in \mathrm{MF}^{(S)}$, such that $n = n_{\mathcal{U}(M)}$.*

Proof. Let $\pi(n) = v \in \mathcal{V}_S$.

If $(r_1, r_2) \in S_v$, take $\beta^0_{r_2, r_1} \in W(k)$, such that $v_p(\beta^0_{r_2 r_1}) = v(r_1, r_2)$.

If $(r_1, r_2) \in S \times S \setminus S_v$, set $\beta^0_{r_2 r_1} = 0$.

Show, that there exists $M \in \mathrm{MF}^{(S)}$ given in notation of n.2.2 by these coefficients $\beta^0_{r_2 r_1}, r_1, r_2 \in S$.

If $r, r' \in S$ and $l_0(r) \geq l_0(r')$, then by proposition of n.2.5.4 $(r, r') \notin S_v$, therefore, $\beta^0_{r' r} = 0$ and the condition b_2) of n.2.2 holds.

To deduce the condition b_1) of n.2.2 set for any $r, r' \in S$

$r \succ r'$, if $n(r, r') = 0$, and $r \not\succ r'$, otherwise, i.e. if $n(r, r') > 0$.

Properties of the function n imply the following properties of the relation $\succ$.

1) $r \not\succ r$ for any $r \in S$;

2) $r_1 \succ r_2, r_2 \succ r_3 \Rightarrow r_1 \succ r_3$ for any $r_1, r_2, r_3 \in S$;

3) $r_1 \succ r_2 \Leftrightarrow r_1(1) \succ r_2(1)$ for any $r_1, r_2 \in S$.

Let $S = \{r_1, \dots, r(h_1 - 1); \dots; r_m, \dots, r(h_m - 1)\}$, c.f. n.2.2. b_1).

Properties 1) and 2) imply existence of strictly minimal element $r_{j_m}(\alpha_0), \alpha_0 \in \mathbb{Z}/h_{j_m}\mathbb{Z}$, i.e. $r_{j_m}(\alpha_0) \not\succ r$ for any $r \in S$. By the property 3) we have $r_{j_m}(\alpha) \succ r$ for all $\alpha \in \mathbb{Z}/h_{j_m}\mathbb{Z}$.

Apply this procedure to the set $S_{j_m} = S\setminus\{r_{j_m}(\alpha) \mid \alpha \in \mathbb{Z}/h_{j_m}\mathbb{Z}\}$. We obtain an index $j_{m-1} \neq j_m$, such that for all $\alpha \in \mathbb{Z}/h_{j_{m-1}}\mathbb{Z}$ and $r \in S_{j_m}$ one has $r_{j_{m-1}}(\alpha) \not\succ r$. Repeating this process we obtain substitution $\begin{pmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{pmatrix}$, such that

if $r = r_{j_a}(\alpha), r' = r_{j_b}(\beta), a \geq b, \alpha \in \mathbb{Z}/h_{j_a}\mathbb{Z}, \beta \in \mathbb{Z}h_{j_b}\mathbb{Z}$, then $r \not\succ r'$, i.e. $n(r,r') > 0$.

If in the above notation $\beta^0_{r'r} \neq 0$, then $(r,r') \in S_v$ and $v_p(\beta^0_{r'r}) = v(r,r') = n(r,r') > 0$, i.e. $\beta^0_{r'r} \in pW(k)$ and condition b_1) holds. If $\beta^0_{r'r} = 0$, then condition b_1) holds by trivial reasons.

Theorem B is proved.

2.5.3. Let G be a formal group of finite height over $W(k)$, $\operatorname{char} k = p > 2$. Then its Tate module $T(G)$ is Fontaine-Laffaille Γ-module with weights 0 and 1.

Assume, that $T(G)$ satisfies conditions C1-C3 of n.1 and denote by $S(G)$ corresponding set of characters $S(T(G))$ of Γ_{tr}. Equivalently, $S(G)$ is a finite subset in $R_p(1) \setminus \{0\}$, where

$$R_p(1) = \{\ r \in R_p \mid l_s(r) = 0 \ \text{ or } \ 1 \ \text{ for all } \ s \in \mathbb{Z}_{\geq 0}\ \},$$

such that $r \in S(G) \Rightarrow r(1) \in S(G)$ and $S(G)$ satisfies the property C5 of n.2.2.

In this case the property d') of n.2.5.2 plays its rôle, iff $\{1/(p-1)\} \subsetneq S(G)$, i.e. if the formal group G contains the multiplicative formal group $\hat{\mathbb{G}}_m$, but $G \neq \hat{\mathbb{G}}_m$.

So, we have the following proposition.

Proposition. *If $S \subset R_p(1) \setminus \{0; 1/(p-1)\}$ satisfies the property C5 of n.2.2, and a function $n : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ satisfies properties a) – d) of n.2.5.2, then there exists a formal group G over $W(k)$ of height $h = |S|$, such that $S(G) = S$ and $n_{T(G)} = n$.*

This proposition means, that if U is Γ-module, such that $S(U) = S$ satisfies assumptions of the above proposition, then its invariant n_U appears in a form $n_{T(G)}$ for some formal group G. We do not study here realization of the second invariant $\mathcal{H}_0(T(G))$ from proposition of n.1.2 except some trivial cases (c.f. n.2.5.4 below).

2.5.4. Assume, that

$$S = \{r, r(1), \dots, r(h-1)\ \},$$

where $r \in R_p(p-2)$ and $h = h(r)$, i.e. the sequence $\{l_s(r)\}_{s\geq 0}$ of p-digits of r has minimal positive period h. Let χ be the character of $s(\Gamma_{tr})$, such that $r(\chi) = r$. By proposition of n.1.1 we have

$\operatorname{ord}\chi = p^h - 1 \ \Rightarrow S$ satisfies the condition C5.

So, in this case we can use proposition of n.1.3 for description of the image of the Galois group Γ in $\operatorname{Aut}_{\mathbb{Z}_p} U$.

Under above assumptions the condition d') coincides with the condition d).

Indeed, let $r_1, r_1 \in S$ be such that $l_0(r_1(i)) \geq l_0(r_2(i))$ for all $i \in \mathbb{Z}$. Take $\alpha \in \mathbb{Z}$, such that $r_2 = r_1(\alpha)$. Then for any $i \in \mathbb{Z}$ the condition d′) implies

$$l_0(r_1(i)) \geq l_0(r_2(i)) = l_0(r_1(i+\alpha)) \geq \cdots \geq l_0(r_1(i+h\alpha)) = l_0(r_1(i)).$$

Therefore, $l_0(r_1(i)) = l_0(r_1(i+\alpha))$ for all $i \in \mathbb{Z}$,. This gives $\alpha \equiv 0 \bmod h$ and $r_2 = r_1$.

So, we have the following proposition.

Proposition. *Let $r \in R_p(p-2)$ be such that $r = l/(p^h - 1)$, where $l \in \mathbb{N}$ and c.g.d.$(l, p^h-1) = 1$, $S = \{\ r, r(1), \ldots, r(h-1)\ \}$ and let $n : \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}$ be such that*

$$n(0) = \min\{\ n(i) + n(-i) \mid i \in \mathbb{Z}/h\mathbb{Z}\ \},$$
$$n(i+j) \leq n(i) + n(j) \quad \text{for all} \quad i, j \in \mathbb{Z}/h\mathbb{Z}.$$

Then there exists $M \in \mathrm{MF}^{(S)}$, such that $n_{\mathcal{U}(M),\chi} = n$ (where χ is the character of Γ_{tr}, such that $r(\chi) = r$).

2.5.5. In notation and assumptions of n.2.5.3 suppose, that $r \in R_p(p-2)$ satisfies assumption C6 of n.3.12 below, i.e. polynomes $l_0(r)X^{p^{h-1}} + \cdots + l_{h-1}(r)X$ and $X^{p^h-1} - 1$ are relatively prime in $\mathbb{F}_p[X]$. By remark of n.3.12 the second invariant $\mathcal{H}_0(\chi)$ of the image $H(M)$ of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} \mathcal{U}(M))$ equals $pW(\mathbb{F}_{p^h})e_{00}$. Therefore, under additional assumption C6 proposition of n.2.5.3 gives complete information about $H(M)$.

We have natural realization of the above assumptions in a following situation.

Let $p > 2$ and G be a 1-dimensional formal group over $W(k)$ of finite height h. Denote by $S(G)$ the set of characters of the group $s(\Gamma_{\mathrm{tr}})$ of the image $H(G)$ of Γ in $\mathrm{Aut}_{\mathbb{Z}_p} T(G)$, where $T(G)$ is Tate module of G. Then tamely ramified character χ_h^* (c.f. n.2.2) belongs to $S(G)$ and $S(G) = \{\ p^i/(p^h-1) \mid 0 \leq i < h\ \}$. Clearly, additional assumption C6 is also satisfied here and we obtain the following proposition.

Proposition. *Let H be a closed subgroup of $\mathrm{Aut}_{\mathbb{Z}_p} W(\mathbb{F}_{p^h})$. Then the following statements are equivalent:*

1) *There exists 1-dimensional formal group G of height h over $W(k)$ and an isomorphism of $\mathbb{Z}_p$-modules $T(G) \simeq W(\mathbb{F}_{p^h})$, which transforms the image $H(G)$ of Γ on H;*

2) *H is an extension of a cyclic group of order relatively prime to p by normal pro-p-group (i.e. it satisfies the condition C1 of n.1) and $H \supset W(\mathbb{F}_{p^h})^*$.*

Remark. This proposition gives positive answer to the question of J.-M. Fontaine from [Fo1] (a special case of this problem was considered in [Na]). We can also use a relation between filtered module associated to the above formal groups G and functional equations of their logarithms, c.f. [Fo2, Ch.5], to give explicit expression for the associated function $n_{T(G),\chi_h^*}$ as follows. Let $l_G(X) \in W_{\mathbb{Q}_p}[[X]]$ be a logarithm of the formal group G, which satisfies the functional equation

$$l_G(X) = X + \frac{1}{p}(\alpha_1 \sigma_* l_G(X^p) + \cdots + \alpha_h \sigma_*^h l_G(X^{p^h}))$$

Here σ_* means action of absolute Frobenius on coefficients of power series, $\alpha_1, \dots ,\alpha_{h-1} \in pW(k)$, and $\alpha_h \in W(k)^*$. Then for any $i \in \mathbb{Z}/h\mathbb{Z}$ we have

$$n_{T(G),\chi_h^*}(i) =$$

$$= \min\{v_p(\alpha_{i_1}) + \dots + v_p(\alpha_{i_s}) \mid s \in \mathbb{N}, 1 \le i_1, \dots , i_s < h, (i_1 + \dots + i_s) \bmod h = i \}.$$

3. Proof of the theorem A.

3.1. Let $M \in \mathrm{MF}^{(S)}$ be given in notation of n.2.2. Choose $r_1, \dots , r_m \in S$, such that

$$S = \{ r_1, \dots , r_1(h_1 - 1); \dots ; r_m, \dots , r_m(h_m - 1) \},$$

where $h_j = h(r_j)$ are (as earlier) minimal positive periods of p-digit expansions of $r_j, 1 \le j \le m$.

Choose $N \in \mathbb{N}$, such that $N \equiv 0 \bmod h_j$ for all $1 \le j \le m$.

Choose $\beta_{(r_j,i),(r_{j'},i')} \in W(k)$, where $1 \le j, j' \le m, i, i' \in \mathbb{Z}/N\mathbb{Z}$, such that for every $r \in S$ one has

$$\sum_{\substack{i \in \mathbf{Z}/N\mathbf{Z} \\ r_j(i)=r}} \beta_{(r_j,i),(r_{j'},i')} = \beta_{r,r_{j'}(i')}$$

and

$$\min\{ v_p(\beta_{(r_j,i),(r_{j'},i')}) \mid i \in \mathbb{Z}/N\mathbb{Z}, r_j(i) = r \} = v_p(\beta_{r,r_{j'}(i')}).$$

Define $M^* \in \mathrm{MF}_f$ as follows.

1) M^* has $W(k)$-basis $\{m_{(r_j,i)} \mid 1 \le j \le m, i \in \mathbb{Z}/N\mathbb{Z} \}$;

2) for $0 \le l < p$ the submodule M^{*l} of filtration on M^* is generated by

$$\{ m_{(r_j,i)} \mid l_i(r_j) \ge l \}$$

(in particular, $m_{(r_j,i)} \in M^{*l_0(r_j(i))} \setminus M^{*l_0(r_j(i))+1}$);

3) for $0 \le l < p$ σ-linear morphisms $\phi_l : M^{*l} \longrightarrow M$ are (uniquelly) defined by relations

$$\phi_{l_{i-1}(r_j)}(m_{(r_j,i-1)}) = m_{(r_j,i)} + \sum_{\substack{1 \leqslant j' \leqslant m \\ i' \in \mathbf{Z}/N\mathbf{Z}}} \beta_{(r_j,i),(r_{j'},i')} m_{(r_{j'},i')}.$$

One can easily check up, that the correspondence

$$i_{M,M^*} : m_r \mapsto \sum_{\substack{i \in \mathbf{Z}/N\mathbf{Z} \\ r_j(i)=r}} m_{(r_j,i)}$$

gives injective morphism $i_{M,M^*} : M \longrightarrow M^*$ in the category MF_f.

3.2. From definition of the functor $\mathcal{U}$ it follows, that the correspondence

$$u \mapsto (m_r(u))_{r \in S} \in \oplus_{r \in S} A_{\mathrm{cris}}$$

gives injective morphism of Γ-modules

$$\kappa : \mathcal{U}(M) \longrightarrow \oplus_{r\in S} A_{\mathrm{cris}}.$$

Also, $W(k)$-linear prolongation $\kappa_{W(k)}$ of κ

$$\kappa_{W(k)} : \mathcal{U}(M) \otimes W(k) \longrightarrow \oplus_{r\in S} A_{\mathrm{cris}}$$

is still injective.

Under the above identification κ $\mathcal{U}(M)$ is identified with $\mathbb{Z}_p[\Gamma]$- module of collections $(u_r)_{r\in S} \in \oplus_{r\in S} A_{\mathrm{cris}}$, such that for every $r \in S$ one has

$$u_r \in A_{\mathrm{cris}}^{l_0(r)}$$

and

$$\phi_{l_0(r(-1))}(u_{r(-1)}) = u_r + \sum_{r'\in S} \beta_{rr'} u_{r'}.$$

Analogously, $\mathcal{U}(M^*)$ can be identified with collections $(u_{(r_j,i)})_{1\leq j\leq m, i\in \mathbf{Z}/N\mathbf{Z}}$, such that for every $1 \leq j \leq m, i \in \mathbb{Z}/N\mathbb{Z}$ one has

$$u_{(r_j,i)} \in A_{\mathrm{cris}}^{l_i(r_j)}$$

and

$$\phi_{l_{i-1}(r_j)}(u_{(r_j,i-1)}) = u_{(r_j,i)} + \sum_{\substack{1\leqslant j'\leqslant m \\ i'\in \mathbf{Z}/N\mathbf{Z}}} \beta_{(r_j,i),(r_{j'},i')} u_{(r_{j'},i')}.$$

Epimorphism $\mathcal{U}(i_{M,M^*}) : \mathcal{U}(M^*) \longrightarrow \mathcal{U}(M)$ and its $W(k)$-linear prolongation are induced by the homomorphism

$$\oplus_{\substack{1\leqslant j\leqslant m \\ i\in \mathbf{Z}/N\mathbf{Z}}} A_{\mathrm{cris}} \longrightarrow \oplus_{r\in S} A_{\mathrm{cris}},$$

such that $(a_{(r_j,i)})_{1\leqslant j\leqslant m, i\in \mathbf{Z}/N\mathbf{Z}} \mapsto (a_r)_{r\in S}$, where $a_r = \sum_{r_j(i)=r} a_{(r_j,i)}$.

If $\mathcal{U}(M) \otimes W(k) = \oplus_\chi U(M)_\chi$ and $\mathcal{U}(M^*) \otimes W(k) = \oplus_\chi \mathcal{U}(M^*)_\chi$ are decompositions of $s(\Gamma_{\mathrm{tr}})$-modules by characters χ of the group $s(\Gamma_{\mathrm{tr}})$, then for every χ we have induced epimorphic map of $W(k)$-modules

$$\mathcal{U}(i_{M,M^*})_\chi : \mathcal{U}(M^*)_\chi \longrightarrow U(M)_\chi.$$

3.3. For $1 \leq j_0, \dots, j_s, \dots \leq m, a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ define objects $M^*(j_0), M^*(j_1, b_1; a_0, j_0), \dots, M^*(j_s, b_s; a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0)$ of the category MF_f as follows.

$M^*(j_0)$ has $W(k)$-basis $\{m(i,j_0) \mid i \in \mathbb{Z}/N\mathbb{Z}\ \}$, for $0 \leq l < p$ its filtration submodule $M(j_0)^{*l}$ is generated by $\{m(i,j_0) \mid l_i(r_{j_0}) \geq l\}$, and σ-linear morphisms $\phi_l : M(j_0)^{*l} \longrightarrow M^*(j_0)$ are uniquelly defined by relations

$$\phi_{l_{i-1}(r_{j_0})}(m(i-1,j_0)) = m(i,j_0).$$

If $s \geq 1$, then $M^*(j_s, b_s; \dots; a_0, j_0)$ has $W(k)$-basis

$$\{m(i, j_l, b_l; \dots; a_0, j_0) \mid 0 \leq l \leq s, i \in \mathbb{Z}/N\mathbb{Z}\},$$

for $0 \leq l' < p$ its filtration submodule $M(j_s, b_s; \dots; a_0, j_0)^{*l'}$ is generated by

$$\{m(i, j_l, b_l; \dots; a_0, j_0) \mid l_i(r_{j_l}) \geq l'\},$$

and σ-linear morphisms $\phi_{l'} : M(j_s, b_s; \dots; a_0, j_0)^{*l'} \longrightarrow M^*(j_s, b_s; \dots; a_0, j_0)$ are (uniquelly) defined by relations

$$\phi_{l_{i-1}(r_{j_l})}(m(i-1, j_l, b_l; \dots; a_0, j_0)) = m(i, j_l, b_l; \dots; a_0, j_0) +$$

$$+\delta(i, b_l)\beta^*_{(r_{j_l}, b_l),(r_{j_{l-1}}, a_{l-1})} m(a_{l-1}, j_{l-1}, b_{l-1}; \dots; a_0, j_0),$$

where $l \geq 1$, δ is Kronecker symbol, and

$$\beta^*_{(r_{j_l}, b_l),(r_{j_{l-1}}, a_{l-1})} = p^{-n^*_M(r_{j_{l-1}}(a_{l-1}), r_{j_l}(b_l))} \beta_{(r_{j_l}, b_l),(r_{j_{l-1}}, a_{l-1})}$$

(if $n^*_M(r_{j_{l-1}}(a_{l-1}), r_{j_l}(b_l)) = +\infty$, we take $\beta^*_{(r_{j_l}, b_l),(r_{j_{l-1}}, a_{l-1})} = 0$).

For any $s \geq 1$ we have natural imbeddings in the category MF_f

$$(*) \qquad M^*(j_{s-1}, b_{s-1}; \dots; a_0, j_0) \longrightarrow M^*(j_s, b_s; \dots; a_0, j_0).$$

If $U^*(j_s, b_s; \dots; a_0, j_0) = \mathcal{U}(M^*(j_s, b_s; \dots; a_0, j_0))$, then we have m projective systems of $\mathbb{Z}_p[\Gamma]$-modules

$$\mathcal{L}_{j_0} = \{U^*(j_s, b_s; \dots; a_0, j_0) \mid j_0 \text{ is fixed }\}, 1 \leq j_0 \leq m,$$

where all connecting morphisms

$$U^*(j_s, b_s; \dots; a_0, j_0) \longrightarrow U^*(j_{s-1}, b_{s-1}; \dots; a_0, j_0)$$

are surjective morphisms of $\mathbb{Z}_p[\Gamma]$-modules, which arise by Fontaine-Laffaille theory from embeddings $(*)$.

3.4. Let $1 \leq j_0 \leq m$, then by arguments of n.3.2 the correspondence

$$\kappa_{j_0} : u^* \mapsto (m(i, j_0)(u^*))_{i \in \mathbf{Z}/N\mathbf{Z}} \in \oplus_{i \in \mathbf{Z}/N\mathbf{Z}} A_{\mathrm{cris}}$$

gives identification of $U^*(j_0)$ with $\mathbb{Z}_p[\Gamma]$-submodule of $\oplus_{i \in \mathbf{Z}/N\mathbf{Z}} A_{\mathrm{cris}}$, which consists of $(u_i)_{i \in \mathbf{Z}/N\mathbf{Z}}$, such that $u_i \in A_{\mathrm{cris}}^{l_i(r_{j_0})}$ and $\phi_{l_{i-1}(r_{j_0})}(u_{i-1}) = u_i$ for all $i \in \mathbb{Z}/N\mathbb{Z}$.
Fix some $u^*(j_0) \in U^*(j_0) \setminus pU^*(j_0)$. If $\kappa_{j_0}(u^*(j_0)) = (u^*(i, j_0))_{i \in \mathbf{Z}/N\mathbf{Z}}$, then

$$\kappa_{j_0}(U^*(j_0)) = \{ \ (w_i u^*(i, j_0))_{i \in \mathbf{Z}/N\mathbf{Z}} \mid w_i \in W(\mathbb{F}_q), \sigma w_i = w_{i+1} \ \},$$

where $q = p^N$.

If $\tau \in s(\Gamma_{\rm tr})$, then $\tau u^*(i,j_0) = \chi_{i,j_0}(\tau)u^*(i,j_0)$, where χ_{i,j_0} is a character of $s(\Gamma_{\rm tr})$ with invariant $r(\chi) = r_{j_0}(i)$.

Indeed, if $\tau \in \Gamma$ and $\kappa_{j_0}(\tau u^*(i,j_0)) = (w_{i,\tau}u^*(i,j_0))_{i\in\mathbb{Z}/N\mathbb{Z}}$, then the correspondence $\tau \mapsto w_{i,\tau}$ gives a continuos homomorphism $\eta_i : \Gamma \longrightarrow W(\mathbb{F}_q)^*$, and $\chi_i = \eta_i|_{s(\Gamma_{\rm tr})}$ is a character of the group $s(\Gamma_{\rm tr})$. It is sufficient to prove, that

$$(*) \qquad \chi \equiv \chi_{i,j_0} \bmod pW(\mathbb{F}_q).$$

If $N = h(r_{j_0}) = h_{j_0}$, then $M^*(j_0)\otimes k = M(r_{j_0})$ is a simple object of the category MF, and the equivalence $(*)$ follows from explicit description of Γ-module $\mathcal{U}(M(r_{j_0})) = U^*(j_0)\otimes\mathbb{F}_p$, n.2.1. If $N \equiv 0 \bmod h_{j_0}$, one can reduce the problem to the above case, because $M^*(j_0)\otimes k$ is isomorphic to the product of N/h_{j_0} copies of $M(r_{j_0})$.

In fact, the above homomorphisms $\eta_i : \Gamma \longrightarrow W(\mathbb{F}_q)^*$ can be calculated in a following way.

Let G_N^{LT} be Lubin-Tate formal group over $W(\mathbb{F}_q)$ with logarithm

$$l(X) = X + X^q/p + \dots + X^{q^s}/p^s + \dots .$$

Action of Γ on the Tate module $T(G_N^{LT})$ of this group is given by continuos homomorphism

$$\eta_{LT} : \Gamma \longrightarrow \mathrm{Aut}(G_h^{LT}) = W(\mathbb{F}_q)^*.$$

If $I_0^{\rm ab}$ is the inertia subgroup of the Galois group of the maximal abelian extension of the quotient field of $W(\mathbb{F}_q)$, then we have a natural projection $\Gamma \longrightarrow I_0^{\rm ab}$ and identification of class field theory $I_0^{\rm ab} = W(\mathbb{F}_q)^*$. In these terms the homomorphism η_{LT} is equal to the composition

$$\eta_{LT} : \Gamma \longrightarrow I_0^{\rm ab} = W(\mathbb{F}_q)^* \xrightarrow{\alpha} W(\mathbb{F}_q)^*,$$

where $\alpha(u) = u^{-1}$, $u \in W(\mathbb{F}_q)^*$.

Let $r = r_{j_0}, M^*(j_0) = M^*(r), u^*(j_0) = u^*, u^*(i,j_0) = u^*(i)$. So, for any $i \in \mathbb{Z}/N\mathbb{Z}$ and $\tau \in \Gamma$, we have $\tau u^*(i) = \eta_i(\tau)u^*(i)$ and $\eta_i(\tau) = \sigma^i\eta_0(\tau)$.

Lemma. $\eta_0 = \prod\limits_{0\leqslant i<N} (\sigma^{-i}\eta_{LT})^{l_i(r)}$.

Proof.

Tate module $T = T(G_N^{LT})$ is Fontaine-Laffaille $\mathbb{Z}_p[\Gamma]$-module, and one can use the following explicit construction of filtered $W(k)$-module $M_0 \in \mathrm{MF}_f$, such that $\mathcal{U}(M_0) = T$.

Let $o = (o_n)_{n\geq 0} \in T$, where $o_n \in G_N^{LT}(\bar{m})$ ($\bar{m}$ is the maximal ideal of the valuation ring $\bar{O}$ of $\bar{K}$), $[p]o_{n+1} = o_n$ for $n \geq 0$ and $o_0 = 0$ (here $[p] = p\,\mathrm{id}_{G_N^{LT}} \in \mathrm{End}\, G_N^{LT}$). If $\hat{o}_n \in A_{\rm cris}$ is a lifting of $o_n \bmod p \in \bar{m} \bmod p\bar{O}$ with respect to the structural epimorphism $A_{\rm cris} \longrightarrow \bar{O}/p\bar{O}$ from definition of $A_{\rm cris}$, then one can show, that the correspondence

$$o \mapsto \lim_{n\to\infty} p^n l(\hat{o}_n)$$

gives well-defined $m_0^{(0)} \in \mathrm{Hom}(T, A^1_{\mathrm{cris}})$, $\sigma^N m_0^0 = p m_0^0$ and

$$M_0 = M_0^0 = \sum_{i \in \mathbb{Z}/N\mathbb{Z}} W(k) m_i^{(0)}, \quad M_0^1 = W(k) m_0^{(0)},$$

where $m_i^{(0)} = \sigma^{\hat{i}} m_0^{(0)}/p$ for $0 < \hat{i} \leq N, \hat{i} \bmod N = i$.

From this construction it follows, that for any $o \in T$ and $\tau \in \Gamma$ one has

$$\tau m_0^{(0)}(o) = \eta_{LT}(\tau) m_0^{(0)}(o).$$

Let $o = (o_n)_{n \geq 0} \in T$ be such that $o_1 \neq 0$. Then $v = m_0^{(0)}(o) \in A^1_{\mathrm{cris}}$, $\tau v = \eta_{LT}(\tau) v$ for all $\tau \in \Gamma$, and $\sigma^N v = pv$.

Now one can check up, that for all $i \in \mathbb{Z}/N\mathbb{Z}$

$$u'(i) = v^{l_i(r)} (\sigma^{-1} v)^{l_{i+1}(r)} \dots (\sigma^{-(N-1)} v)^{l_{i+N-1}(r)} \in A^{l_i(r)}_{\mathrm{cris}},$$

$v_p(u'(i)) = 0$, and $\phi_{l_{i-1}(r)}(u'(i-1)) = u'(i)$.

This gives $u' = (u'(i))_{i \in \mathbb{Z}/N\mathbb{Z}} \in \kappa(U(M^*(r))$, $u'(0) = wu^*(0)$ for some $w \in W(\mathbb{F}_q)^*$, and $\tau u'(0) = \eta_0(\tau) u'(0)$ for $\tau \in \Gamma$. On the other hand,

$$\tau u'(0) = (\tau v)^{l_0(r)} (\sigma^{-1} \tau v)^{l_1(r)} \dots (\sigma^{-(N-1)} \tau v)^{l_{N-1}(r)} =$$

$$= \eta_{LT}^{l_0(r) + \sigma^{-1} l_1(r) + \dots + \sigma^{-(N-1)} l_{N-1}(r)}(\tau) u'(0).$$

Lemma is proved.

3.5. We have the following

Proposition. *For $1 \leq j_0, \dots, j_s, \dots \leq m$, $i, a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ there exist a family of elements $u(i, j_0), \dots, u(i, j_s, b_s; \dots; a_0, j_0), \dots \in A_{\mathrm{cris}}$, such that*

1) *$u(i, j_0) \in A^{l_i(r_{j_0})}_{\mathrm{cris}}$ and for $s \geq 1$*

$$u(i, j_s, b_s; \dots; a_0, j_0) \in A^{l_i(r_{j_s})}_{\mathrm{cris}};$$

2) *$\phi_{l_{i-1}(r_{j_0})}(u(i-1, j_0)) = u(i, j_0)$ and for $s \geq 1$*

$$\phi_{l_{i-1}(r_{j_s})}(u(i-1, j_s, b_s; \dots; a_0, j_0)) = u(i, j_s, b_s; \dots; a_0, j_0) +$$

$$+ \delta(i, b_s) \beta_{(r_{j_s}, b_s), (r_{j_{s-1}}, a_{s-1})} u(a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0);$$

3) *for any $\tau \in s(\Gamma_{\mathrm{tr}})$*

$$\tau u(i, j_s, b_s; \dots; a_0, j_0) = \chi_{i, b_s, \dots, a_0}(\tau) u(i, j_s, b_s; \dots; a_0, j_0),$$

where $\chi_{i, b_s, \dots, a_0}$ is a character of $s(\Gamma_{\mathrm{tr}})$ with invariant

$$r(\chi_{i, b_s, \dots, a_0}) = r_{j_0}(i - b_s + a_{s-1} - \dots - b_1 + a_0);$$

4) $v_p(u(i,j_0))=0$ *and for* $s\geq 1$

$$v_p(u(i,j_s,b_s;\dots;a_0,j_0)\geq n^*_M(r_{j_{s-1}}(a_{s-1}),r_{j_s}(b_s))+\dots+n^*_M(r_{j_0}(a_0),r_{j_1}(b_1)).$$

Proof.

Let $1\leq j_0\leq m$ and consider the projective system $\mathcal{L}_{j_0}$ from n.3.3. We want to construct a compatible system

$$u^*(j_s,b_s;\dots;a_0,j_0)\in U^*(j_s,b_s;\dots;a_0,j_0),$$

such that $u^*(j_0)\in U^*(j_0)\setminus pU^*(j_0)$ (c.f. n.3.4), and if

$$u^*(i,j_s,b_s;\dots;a_0,j_0)=m(i,j_s,b_s;\dots;a_0,j_0)(u^*(j_s,b_s;\dots;a_0,j_0))\in A_{\text{cris}},$$

then for any $\tau\in s(\Gamma_{\text{tr}})$ one has

$$\tau u^*(i,j_s,b_s;\dots;a_0,j_0)=\chi_{i,b_s,\dots,a_0}(\tau)u^*(i,j_s,b_s;\dots;a_0,j_0).$$

In fact, the case $s=0$ was considered in n.3.4.

By induction we can assume, that these points are constructed for all $l<s$.

Take $\hat{u}(j_s,b_s;\dots;a_0,j_0)\in U^*(j_s,b_s;\dots;a_0,j_0)$ such that

$$\hat{u}(j_s,b_s;\dots;a_0,j_0)\mapsto u^*(j_{s-1},b_{s-1};\dots;a_0,j_0)$$

under epimorphism $U^*(j_s,b_s;\dots;a_0,j_0)\longrightarrow U^*(j_{s-1},b_{s-1};\dots;a_0,j_0)$.

Let $\hat{u}(i,j_s,b_s;\dots;a_0,j_0)=m(i,j_s,b_s;\dots;a_0,j_0)(\hat{u}(j_s,b_s;\dots;a_0,j_0))\in A_{\text{cris}}$. Then

$$\hat{u}(i,j_s,b_s;\dots;a_0,j_0)\in A_{\text{cris}}^{l_i(r_{j_s})}$$

and

$$(*)\qquad \phi_{l_{i-1}(r_{j_s})}(\hat{u}(i-1,j_s,b_s;\dots;a_0,j_0))=\hat{u}(i,j_s,b_s;\dots;a_0,j_0)+$$
$$+\delta(i,b_s)\beta^*_{(r_{j_s},b_s),(r_{j_{s-1}},a_{s-1})}u^*(j_{s-1},b_{s-1};\dots;a_0,j_0).$$

Take decomposition by χ-components

$$\hat{u}(i,j_s,b_s;\dots;a_0,j_0)=\sum_\chi\hat{u}(i,j_s,b_s;\dots;a_0,j_0)_\chi,$$

where χ runs over the set of characters of the group $s(\Gamma_{\text{tr}})$. Clearly, non-zero components can appear only for characters χ, such that $r(\chi)\in S$ (in particular, one has for such characters $\sigma^N\chi=\chi$).

Set

$$u^*(i,j_s,b_s;\dots;a_0,j_0)=u(i,j_s,b_s;\dots;a_0,j_0)_{\chi_{i,b_s,\dots,a_0}}.$$

Then comparison of χ-components of the above equality $(*)$ gives

$$\phi_{l_{i-1}(r_{j_s})}(u^*(i-1,j_s,b_s;\dots;a_0,j_0))=u^*(i,j_s,b_s;\dots;a_0,j_0)+$$

$$+\delta(i,b_s)\beta^*_{(r_{j_s},b_s),(r_{j_{s-1}},a_{s-1})}u^*(j_{s-1},b_{s-1};\dots;a_0,j_0).$$

Therefore, there exists $u^*(j_s,b_s;\dots;a_0,j_0)\in U^*(j_s,b_s;\dots;a_0,j_0)$, such that

$$m(i,j_s,b_s;\dots;a_0,j_0)(u^*(j_s,b_s;\dots;a_0,j_0))=u^*(i,j_s,b_s;\dots;a_0,j_0).$$

It is easy to see, that $u^*(j_s,b_s;\dots;a_0,j_0)\mapsto u^*(j_{s-1},b_{s-1};\dots;a_0,j_0)$, and by construction these points satisfy properties from the beginning of this proof.

Now, the relation

$$u(i,j_s,b_s;\dots;a_0,j_0)=$$

$$=p^{n^*_M(r_{j_{s-1}}(a_{s-1}),r_{j_s}(b_s))+\dots+n^*_M(r_{j_0}(a_0),r_{j_1}(b_1))}u^*(i,j_s,b_s;\dots;a_0,j_0),$$

gives the family of elements of A_{cris}, which satisfy the properties of our proposition.

3.6. For $1\le j_0\le m$ consider the collection

$$u^{(j_0)}=(u^{(j_0)}_{(r_j,i)})\in\oplus_{\substack{1\leqslant j\leqslant m\\ i\in\mathbf{Z}/N\mathbf{Z}}}(A_{\mathrm{cris}})_{(r_j,i)},$$

where

$$u^{(j_0)}_{(r_j,i)}=\sum u(i,j,b_s;a_{s-1},j_{s-1},b_{s-1};\dots;a_0,j_0),$$

and the above sum is taken for all $s\ge 0$, $1\le j_1,\dots j_{s-1}\le m$ and $b_s,a_{s-1},\dots,b_1,a_0\in\mathbb{Z}/N\mathbb{Z}$.

One can easily check up, that

$$u^{(j_0)}\in\kappa(\mathcal{U}(M^*)).$$

for any $1\le j_0\le m$.

More generally, if $w\in W(\mathbb{F}_q)$, $q=p^N$, let

$$w*u^{(j_0)}=(w*u^{(j_0)}_{(r_j,i)})_{1\le j\le m,i\in\mathbf{Z}/N\mathbf{Z}},$$

where

$$w*u^{(j_0)}_{(r_j,i)}=\sum(\sigma^{\alpha(i,b_s,\dots,a_0)}w)u(i,j,b_s;\dots;a_0,j_0)$$

and the above sum is taken for all $s\ge 0$, $1\le j_1,\dots,j_{s-1}\le m$, $b_s,a_{s-1},\dots,b_1,a_0\in\mathbb{Z}/N\mathbb{Z}$ and $\alpha(i,b_s,\dots,a_0)=i-b_s+a_{s-1}-\dots-b_1+a_0$.

Then

$$\kappa(\mathcal{U}(M^*))=\{\sum_{1\le j_0\le m}w_{j_0}*u^{(j_0)}\mid w_1,\dots,w_m\in W(\mathbb{F}_q)\ \}.$$

For $1\le j_0,j\le m$, $i_0,i\in\mathbb{Z}/N\mathbb{Z}$, set

$$u^{(j_0,i_0)}_{(j,i)}=\sum u(i,j_s,b_s;\dots;a_0,j_0),$$

where the above sum is taken for all collections $(i, j_s, b_s; \dots; a_0, j_0)$, such that $j_s = j$ and $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

Then

$$u^{(j_0)}_{(r_j,i)} = \sum_{i_0 \in \mathbf{Z}/N\mathbf{Z}} u^{(j_0,i_0)}_{(j,i)},$$

one has for any $w \in W(\mathbb{F}_q)$

$$w * u^{(j_0)}_{(r_j,i)} = \sum_{i_0 \in \mathbf{Z}/N\mathbf{Z}} (\sigma^{i_0} w) u^{(j_0,i_0)}_{(j,i)},$$

and for any $\tau \in s(\Gamma_{\mathrm{tr}})$

$$\tau u^{(j_0)}_{(r_j,i)} = \sum_{i_0 \in \mathbf{Z}/N\mathbf{Z}} \chi_{j_0,i_0}(\tau) u^{(j_0,i_0)}_{(j,i)},$$

where χ_{j_0,i_0} is the character of $s(\Gamma_{\mathrm{tr}})$ with invariant $r(\chi_{j_0,i_0}) = r_{j_0}(i_0)$.

In the above notation $\kappa(\mathcal{U}(M^*))$ is Γ-module of collections

$$(u^*_{(j,i)}) \in \oplus_{\substack{1 \leqslant j \leqslant m \\ i \in \mathbf{Z}/N\mathbf{Z}}} (A_{\mathrm{cris}})_{(r_j,i)},$$

such that

$$u^*_{(j,i)} = \sum_{\substack{i_0 \in \mathbf{Z}/N\mathbf{Z} \\ 1 \leqslant j_0 \leqslant m}} (\sigma^{i_0} w_{j_0}) u^{(j_0,i_0)}_{(j,i)},$$

where $w_1, \dots, w_m$ run over $W(\mathbb{F}_q)$.

Let χ be a character of $s(\Gamma_{\mathrm{tr}})$, such that $r(\chi) \in S$. Then there exist unique $1 \le j_\chi \le m$ and $i_\chi \in \mathbb{Z}/h_{j_\chi}\mathbb{Z}$, such that $r(\chi) = r_{j_\chi}(i_\chi)$. In these terms $\kappa_{W(k)}$ identifies $\mathcal{U}(M^*)_\chi$ with $W(k)$-submodule of $\oplus_{j,i}(A_{\mathrm{cris}})_{(r_j,i)}$, which consists of $(u^*_{\chi,(j,i)})$, such that

$$u^*_{\chi,(j,i)} = \sum_{i_0 \bmod h_{j_\chi} = i_\chi} (\sigma^{i_0} w_{j_\chi}) u^{(j_\chi,i_0)}_{(j,i)}$$

(here w_{j_χ} runs over $W(\mathbb{F}_q)$). This module also is generated by N/h_{j_χ} elements

$$u^{*(i_0)}_\chi = (u^{(j_\chi,i_0)}_{(j,i)})_{\substack{1 \leqslant j \leqslant m, \\ i \in \mathbf{Z}/N\mathbf{Z}}}$$

where $i_0 \in \mathbb{Z}/N\mathbb{Z}$ is such that $i_0 \bmod h_{j_\chi} = i_\chi$.

Use description of the epimorphism $\mathcal{U}(i_{M,M^*})_\chi : \mathcal{U}(M^*)_\chi \longrightarrow \mathcal{U}(M)_\chi$ from n.3.2. This gives generators $u^{(i_0)}_\chi$ of $W(k)$-module $(\kappa_{W(k)}\mathcal{U}(M))_\chi$ in a form

$$u^{(i_0)}_\chi = (u^{(i_0)}_r)_{r \in S} \in \oplus_{r \in S}(A_{\mathrm{cris}})_r,$$

where $i_0 \in \mathbb{Z}/N\mathbb{Z}$, $i_0 \bmod h_{j_\chi} = i_\chi$ and

$$(*) \qquad u^{(i_0)}_r = \sum_{r_j(i) = r} u^{(j_\chi,i_0)}_{(j,i)}$$

for any $r \in S$.

3.7. Let $1 \le j_0 \le m$, $\tau \in \Gamma$. Then for any $i \in \mathbb{Z}/N\mathbb{Z}$ we have

$$\tau u(i, j_0) = w_{(j_0),\tau} * u(i, j_0) (= \sigma^i w_{(j_0),\tau} u(i, j_0)),$$

where $w_{(j_0),\tau} \in W(\mathbb{F}_q)^*$, c.f. n.3.4.

The following lemma can be easily proved by induction on $s \ge 0$.

Lemma. *For $1 \le j_0, j_1, \dots, j_s, \dots \le m$, $a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ and $\tau \in \Gamma$, there exist $w_{(j_s,b_s;\dots;a_0,j_0),\tau} \in W(\mathbb{F}_q)$, such that*

1) *for any $i \in \mathbb{Z}/N\mathbb{Z}$ one has*

$$\begin{aligned}\tau u(i, j_s, b_s; \dots; a_0, j_0) = w_{(j_0),\tau} * u(i, j_s, b_s; \dots; a_0, j_0) + \dots +\\ + w_{(j_l,b_l;\dots;a_0,j_0),\tau} * u(i, j_s, b_s; \dots; a_l, j_l) + \dots +\\ + w_{(j_s,b_s;\dots;a_0,j_0),\tau} * u(i, j_s);\end{aligned}$$

2) $v_p(w_{(j_s,b_s;\dots;a_0,j_0),\tau}) \ge n^*_M(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) + \dots + n^*_M(r_{j_0}(a_0), r_{j_1}(b_1))$.

Remark. As in the above n.3.6 we use the notation

$$w * u(i, j_s, b_s; \dots; a_l, j_l) = (\sigma^{i-b_s+\dots+a_l} w) u(i, j_s, b_s; \dots; a_l, j_l).$$

Use this statement to set

$$w^{(j_0,i_0)}_{(j,i),\tau} = \sum w_{(j_s,b_s;\dots;a_0,j_0),\tau},$$

where the above sum is taken for all collections $(j_s, b_s; \dots; a_0, j_0)$, such that $j_s = j$ and $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

In this notation the above lemma gives the following proposition.

Proposition. *For any $1 \le j_0, j \le m, i_0, i \in \mathbb{Z}/N\mathbb{Z}$ and $\tau \in \Gamma$ there exist $w^{(j_0,i_0)}_{(j,i),\tau} \in W(\mathbb{F}_q)$, such that*

$$\tau u^{(j_0,i_0)}_{(j,i)} = \sum_{\substack{1 \leqslant j_1 \leqslant m \\ i_1 \in \mathbb{Z}/N\mathbb{Z}}} (\sigma^{i_1} w^{(j_0,i_0)}_{(j_1,i_1),\tau}) u^{(j_1,i_1)}_{(j,i)}; \tag{1}$$

$$v_p(w^{(j_0,i_0)}_{(j,i),\tau}) \ge A^{(j_0,i_0)}_{(j,i)}, \tag{2}$$

where $A^{(j_0,i_0)}_{(j,i)}$ is the minimal value of sums

$$n^*_M(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) + \dots + n^*_M(r_{j_0}(a_0), r_{j_1}(b_1))$$

under restrictions $j_s = j$ and $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

Let $u^{(i_0)}_\chi$ be generators of $(\kappa_{W(k)}\mathcal{U}(M))_\chi$ from n.3.6. Then the formula $(*)$ of n.3.6 gives the following corollary.

Corollary. *For every $\tau \in \Gamma$, character χ of the group $s(\Gamma_{\rm tr})$, such that $r(\chi) = r_{j_\chi}(i_\chi)$, and $i_0 \in \mathbb{Z}/N\mathbb{Z}$ one has*

$$\tau u_\chi^{(i_0)} = \sum_{\chi_1, i_1} w^{(j_\chi, i_0)}_{(j_{\chi_1}, i_1), \tau} * u^{(i_1)}_{\chi_1},$$

where χ_1 runs over all characters of $s(\Gamma_{\rm tr})$, such that $r(\chi_1) \in S$, and i_1 runs over $\mathbb{Z}/N\mathbb{Z}$, such that $r_{j_{\chi_1}}(i_1) = r(\chi_1)$.

3.8. Consider the function $n = n_U : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ for $\mathbb{Z}_p[\Gamma]$-module $U = \mathcal{U}(M)$, which was defined in n.1.2 (we use identification of characters of the group $s(H_1)$ with characters of $s(\Gamma_{\rm tr})$, which are given by their invariants $r(\chi) \in S$).

Let $n_M : S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ be the function from n.2.3.

Proposition. *For any $r, r_0 \in S$ one has*

$$n_U(r, r_0) \geq n_M(r, r_0).$$

Proof. If $r = r_0$, then

$$n_U(r, r) = \min\{\ n_U(r, r_1) + n_U(r_1, r) \mid r_1 \in S, r_1 \neq r\ \}$$

by definition, and

$$n_M(r, r) = \min\{\ n_M(r, r_1) + n_M(r_1, r) \mid r_1 \in S, r_1 \neq r\ \},$$

because $n_M^*(r, r) = +\infty$. So, we can assume $r \neq r_0$.

If $r = r_j(i), r_0 = r_{j_0}(i_0)$, where $1 \leq j, j_0 \leq m$, $i, i_0 \in \mathbb{Z}/N\mathbb{Z}$, then corollary of n.3.7 gives

$$n_U(r_0, r) \geq \min\{\ v_p(w^{(j_0, i_0)}_{(j,i),\tau}) \mid r_0 = r_{j_0}(i_0), r = r_j(i)\ \}.$$

Now proposition of n.3.7 implies, that $n_U(r_0, r)$ is not less, than the minimal value of

$$(*) \qquad n_M^*(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) + \cdots + n_M^*(r_{j_0}(a_0), r_{j_1}(b_1)),$$

where $(j_s, b_s; \ldots; a_0, j_0)$ is arbitrary collection, such that $j_s = j$ and $i - i_0 = b_s - a_{s-1} + \cdots + b_1 - a_0$.

Assume, that the collection $(j_s, b_s; \ldots; a_0, j_0)$ with the above restrictions gives the minimal value of the sum $(*)$. Then the property $n_M^*(r_1(1), r_2(1)) = n_M^*(r_1, r_2)$ implies the following equalities

$$n_M^*(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) = n_M^*(r^{(1)}, r),$$

$$n_M^*(r_{j_{s-2}}(a_{s-2}), r_{j_{s-1}}(b_{s-1})) = n_M^*(r^{(2)}, r^{(1)}),$$

$$\cdots\cdots\cdots\cdots$$

$$n^*_M(r_{j_0}(a_0), r_{j_1}(b_1)) = n^*_M(r^{(s)}, r^{(s-1)}),$$

where $r^{(1)} = r_{j_{s-1}}(i_0 + a_{s-1} - b_s), r^{(2)} = r_{j_{s-2}}(i_0 + a_{s-2} + a_{s-1} - b_{s-1} + b_s),$

$$\dots, r^{(s-1)} = r_{j_1}(i_0 + a_1 + \dots + a_{s-2} - b_2 - \dots - b_{s-1}),$$

$$r^{(s)} = r_{j_0}(i_0 + a_0 + \dots + a_{s-1} - b_1 - \dots - b_s) = r_{j_0}(i_0) = r_0.$$

Therefore,

$$n_U(r_0, r) \geq n^*_M(r^{(1)}, r) + n^*_M(r^{(2)}, r^{(1)}) + \dots + n^*_M(r_0, r^{(s-1)}) \geq n_M(r_0, r)$$

by definition of the function n_M.

Proposition is proved.

3.9. Consider the graph $v_M \in \mathcal{V}_S$ of the function n_M, c.f. n.2.4.

Suppose $(r^0, r^1) \in S_{v_M} \subset S \times S$. By proposition of n.2.4.4, $r^0 \neq r^1$. By the definition of the map $\pi : \mathcal{F}_S \longrightarrow \mathcal{V}_S$, we have $v_M(r^0, r^1) = n_M(r^0, r^1)$ and, obviously,

$$v_M(r^0, r^1) = n^*_M(r^0, r^1) = \min\{ v_p(\beta_{r^1(i)r^0(i)}) \mid i \in \mathbb{Z} \}.$$

Let $S(r^0) = \{r^0(i) \mid i \in \mathbb{Z}\} \subset S$ and $S(r^1) = \{r^1(i) \mid i \in \mathbb{Z}\} \subset S$.

Denote by j^0, j^1 uniquelly defined indices from $[1, m]$, such that $r_{j^0} \in S(r^0)$ and $r_{j^1} \in S(r^0)$.

Introduce $M(r^1, r^0) \in \mathrm{MF}_f$, such that

a) $M(r^1, r^0)$ is a free $W(k)$-module with basis

$$\{ m^0_r \mid r \in S(r^0) \} \cup \{ m^1_r \mid r \in S(r^1) \};$$

b) for $0 \leq l < p$ its filtration submodule $M(r^1, r^0)^l$ is generated by

$$\{ m^0_r \mid r \in S(r^0), l_0(r) \geq l \} \cup \{ m^1_r \mid r \in S(r^1), l_0(r) \geq l \};$$

c) σ-linear morphisms ϕ_l, $0 \leq l < p$, are (uniquelly) defined by relations

$$\phi_{l_0(r(-1))} m^0_{r(-1)} = m^0_r, \text{ for } r \in S(r^0),$$

$$\phi_{l_0(r(-1))} m^1_{r(-1)} = m^1_r + \sum_{(r', r) \in S_{(r^0, r^1)}} \beta^*_{rr'} m^0_{r'},$$

for $r \in S(r^1)$, where

$$S_{(r^0, r^1)} = \{ (r^0(i), r^1(i)) \mid i \in \mathbb{Z} \} \subset S(r^0) \times S(r^1) \subset S \times S,$$

$\beta^*_{rr'} = p^{-v_M(r^0, r^1)} \beta_{rr'}$, if $(r', r) \in S_{(r^0, r^1)}$, and $\beta^*_{rr'} = 0$, otherwise.

3.10. Let χ^1, χ^0 be characters of the group Γ_{tr}, such that $r(\chi^1) = r^1$ and $r(\chi^0) = r^0$. Clearly, $\chi^1 \neq \chi^0$.

Proposition. *In notation and assumption of n.3.9 the following conditions are equivalent*

a) $n_U(r^0,r^1)\le v_M(r^0,r^1)$;

b) *there exists* $u\in\mathcal{U}(M(r^1,r^0))$ *and* $\tau_0\in\Gamma$, *such that*

$$(\tau_0 u_{\chi^0})_{\chi^1}\notin p\mathcal{U}(M(r^1,r^0))_{\chi^1};$$

c) *for some* $w_0\in W(\mathbb{F}_q)$ *and* $\tau_0\in\Gamma$

$$\sum_{i^0,i^1,b_1,a_0}(\sigma^{i^0}w_0)(\sigma^{i^1}w_{(j^1,b_1;a_0,j^0),\tau_0})u(i^1,j^1)\notin p^{v_M(r^0,r^1)+1}A_{\mathrm{cris}},$$

where the sum is taken for all $i^0,i^1,b_1,a_0\in\mathbb{Z}/N\mathbb{Z}$, *such that* $i^1-i^0=b_1-a_0$, $r_{j^0}(i^0)=r^0,r_{j^1}(i^1)=r^1$.

Proof.

3.10.1. The condition a) is equivalent to existence of $u\in U=\mathcal{U}(M)$ and $\tau_0\in\Gamma$, such that

$$(\tau_0 u_{\chi^0})_{\chi^1}\notin p^{v_M(r^0,r^1)+1}U_{\chi^1}.$$

In notation of n.3.6 this is equivalent to existence of

$$u^*=\sum_{1\le j_0\le m}w_{j_0}u^{(j_0)}\in\mathcal{U}(M^*),$$

such that the image of $(\tau_0 u^*_{\chi^0})_{\chi^1}$ in U_{χ^1} does not belong to $p^{v_M(r^0,r^1)+1}U_{\chi^1}$.

In notation of nn. 3.6-3.7 we have

1) $u^*_{\chi^0}=(u^*_{\chi^0,(j,i)})$, where

$$u^*_{\chi^0,(j,i)}=\sum_{i^0}(\sigma^{i^0}w_{j_0})u^{(j^0,i^0)}_{(j,i)},$$

and the sum is taken for all $i^0\in\mathbb{Z}/N\mathbb{Z}$, such that $r_{j^0}(i^0)=r^0$.

2) $\tau_0 u^*_{\chi^0}=(\tau_0 u^*_{\chi^0,(j,i)})$, where

$$\tau_0 u^*_{\chi^0,(j,i)}=\sum_{i^0,j_1,i_1}(\sigma^{i^0}w_0)(\sigma^{i_1}w^{(j^0,i^0)}_{(j_1,i_1),\tau_0})u^{(j_1,i_1)}_{(j,i)},$$

and the sum is taken for all $1\le j_1\le m$, $i_1\in\mathbb{Z}/N\mathbb{Z}$ and all $i^0\in\mathbb{Z}/N\mathbb{Z}$, such that $r_{j^0}(i^0)=r^0$.

3) $(\tau_0 u^*_{\chi^0})_{\chi^1}=(u^*_{\chi^0,\chi^1,(j,i)})$, where

$$u^*_{\chi^0,\chi^1,(j,i)}=\sum_{i^0,i^1}(\sigma^{i^0}w_0)(\sigma^{i^1}w^{(j^0,i^0)}_{(j^1,i^1),\tau_0})u^{(j^1,i^1)}_{(j,i)},$$

and the sum is taken for all $i^0,i^1\in\mathbb{Z}/N\mathbb{Z}$, such that $r_{j^0}(i^0)=r^0$ and $r_{j^1}(i^1)=r^1$.

Let $w_{(j_s,b_s;\dots;a_0,j_0),\tau_0}$ be some summand from the expression for $w^{(j^0,i^0)}_{(j^1,i^1),\tau_0}$ from n.3.7. Because of $(r^0,r^1)\in S_{v_M}$ and of the part 2) of lemma of n.3.7, we have:

$$w_{(j_s,b_s;\dots;a_0,j_0),\tau_0}\in p^{v_M(r^0,r^1)}W(\mathbb{F}_q)$$

and, if $s\geq 2$, then

$$w_{(j_s,b_s;\dots;a_0,j_0),\tau_0}\in p^{v_M(r^0,r^1)+1}W(\mathbb{F}_q).$$

Therefore,

$$w^{(j^0,i^0)}_{(j^1,i^1),\tau_0}\equiv\sum_{\substack{b_1,a_0\in\mathbf{Z}/N\mathbf{Z}\\ b_1-a_0=i^1-i^0}} w_{(j^1,b_1;a_0,j^0),\tau_0}\bmod p^{v_M(r^0,r^1)+1}.$$

From the property $n_M(r,r)\geq 1$ and construction of elements $u^{(j^1,i^1)}_{(j,i)}$ it follows, that

$$u^{(j^1,i^1)}_{(j^1,i)}\equiv u(i,j^1)\delta(i,i^1)\bmod pA_{\mathrm{cris}}.$$

By these arguments we obtain from the above formula 3), that

$$u^*_{\chi^0,\chi^1,(j^1,i)}\equiv$$

$$\equiv\sum_{i^0,i^1,b_1,a_0}(\sigma^{i^0}w_{j^0})(\sigma^{i^1}w_{(j^1,b_1;a_0,j^0),\tau_0})u(i,j^1)\delta(i,i^1)\bmod p^{v_M(r^0,r^1)+1}A_{\mathrm{cris}},$$

where the sum is taken for all $i^0,i^1,b_1,a_0\in\mathbb{Z}/N\mathbb{Z}$, such that $i^1-i^0=b_1-a_0$, $r_{j^0}(i^0)=r^0$, $r_{j^1}(i^1)=r^1$.

Now use formulae from n.3.2 to obtain, that the value of $m_r\in M$ on the image of $(\tau_0u^*_{\chi^0})_{\chi^1}$ in $\mathcal{U}(M)_{\chi^1}$ is 0, if $r\neq r^1$, and coincides with the expression of the part c) of our proposition, if $r=r^1$. So, a) and c) are equivalent.

3.10.2. Consider the elements

$$u(i,j^0),u(i,j^1),u^*(i,j^1,b_1;a_0,j^0)=p^{-n^*_M(r^0,r^1)}u(i,j^1,b_1;a_0,j^0)\in A_{\mathrm{cris}}$$

from n.3.5. Proceeding as in n.3.6, we obtain the following description of elements of the Γ-module $\mathcal{U}(M(r^0,r^1))$.

For any $u\in\mathcal{U}(M(r^1,r^0))$ there exist $w_0,w_1\in W(\mathbb{F}_q)$, such that

if $r\in S(r^0)$, then

$$m^0_r(u)=\sum_{\substack{i\in\mathbf{Z}/N\mathbf{Z}\\ r_{j^0}(i)=r}}(\sigma^iw_0)u(i,j^0);$$

if $r \in S(r^1)$, then

$$m_r^1(u) = \sum_{\substack{i \in \mathbf{Z}/N\mathbf{Z} \\ r_{j^1}(i)=r}} (\sigma^i w_1) u(i, j^1) + \sum_{i, a_0, b_1} (\sigma^{i-b_1+a_0} w_0) u^*(i, j^1, b_1; a_0, j^0),$$

where the last sum is taken for all $i, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$, such that $r_{j^1}(i) = r$ and

$$(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}.$$

For the χ^0-component u_{χ^0} of the point u we have

if $r \in S(r^0)$, then

$$m_r^0(u_{\chi^0}) = \delta(r, r^0) \sum_{\substack{i \in \mathbf{Z}/N\mathbf{Z} \\ r_{j^0}(i)=r}} (\sigma^i w_0) u(i, j^0);$$

if $r \in S(r^1)$, then

$$m_r^1(u_{\chi^0}) = \delta(r, r^0) \sum_{\substack{i \in \mathbf{Z}/N\mathbf{Z} \\ r_{j^1}(i)=r}} (\sigma^i w_1) u(i, j^1) + \sum_{i^0, i, a_0, b_1} (\sigma^{i_0} w_0) u^*(i, j^1; a_0, j^0),$$

where the last sum is taken for all $i^0, i, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$, such that $i^0 = i - b_1 + a_0$, $r_{j^0}(i^0) = r^0$, $r_{j^1}(i) = r$ and $(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}$.

Now we can use, that $\chi^0 \neq \chi^1$ and $\tau_0 u^*(i, j^1, b_1; a_0, j^0) =$

$$= (\sigma^{i-b_1+a_0} w_{(j^0), \tau_0}) u^*(i, j^1, b_1; a_0, j^0) + (\sigma^i w^*_{(j^1, b_1; a_0, j^0), \tau_0}) u(i, j^1),$$

where $\tau_0 \in \Gamma$ and

$$(*) \qquad w^*_{(j^1, b_1; a_0, j^0), \tau_0} = p^{-n^*_M(r^0, r^1)} w_{(j^1, b_1; a_0, j^0), \tau_0},$$

to obtain the following description of the point $(\tau_0 u_{\chi^0})_{\chi^1}$:

if $r \in S(r^0)$, then $m_r^0((\tau_0 u_{\chi^0})_{\chi^1}) = 0$;

if $r \in S(r^1)$, then

$$(**) \qquad m_r^1((\tau_0 u_{\chi^0})_{\chi^1}) = \delta(r, r^1) \sum_{i^0, i^1, a_0, b_1} (\sigma^{i^0} w_0)(\sigma^{i^1} w^*_{(j^1, b_1; a_0, j^0), \tau_0}) u(i^1, j^1),$$

where the sum is taken for all $i^0, i^1, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$, such that $i^0 = i^1 - b_1 + a_0$, $r_{j^0}(i^0) = r^0$, $r_{j^1}(i^1) = r^1$ (we use, that the condition $(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}$ is now a consequence of other ones, because $r_{j^1}(b_1) = r^1(b_1 - i^1)$, $r_{j^0}(a_0) = r^0(a_0 - i^0)$ and $b_1 - i^1 = a_0 - i^0$).

So, the part b) of our proposition is equivalent to existence of $w_0 \in W(\mathbb{F}_q)$ and of $\tau_0 \in \Gamma$, such that the right hand side of $(**)$ does not belong to pA_{cris} for $r = r^1$. But this is equivalent to the part c) of our proposition because of the above relation $(*)$.

Proposition is proved.

3.11. In notation and assumptions of n.3.9 we have the following proposition.

Proposition. *The statement of the part* b) *of proposition 3.10 is valid.*

Clearly, the above proposition and propositions of nn.3.8 and 2.4.3 imply our theorem.

Proof of proposition.

This statement uses only the structure of $\mathbb{F}_p[\Gamma]$-module $\mathcal{U}(M(r^1,r^0))\otimes\mathbb{F}_p = U_1(r^1,r^0)$. Galois modules of this kind were studied in details (as important step in description of all annihilated by p subquotients of Fontaine-Laffaille modules) in [Ab2]. So, we give only a sketch of the proof.

3.11.1. In the category MF we have a natural exact sequence

$$(*)\qquad 0\longrightarrow M(r^0)\longrightarrow M(r^1,r^0)\otimes k\longrightarrow M(r^1)\longrightarrow 0,$$

where $M(r^1), M(r^0)$ are simple objects of MF, c.f. n.2.2. This gives exact sequence of $\mathbb{F}_p[\Gamma]$-modules

$$(**)\qquad 0\longrightarrow H^1\longrightarrow U_1(r^1,r^0)\longrightarrow H^0\longrightarrow 0,$$

where H^1 and H^0 are simple $\mathbb{F}_p[\Gamma]$-modules with sets of characters $S(r^1)$ and $S(r^0)$, respectfully. The extension $(**)$ is not trivial, because the above extension $(**)$ is not trivial in the category MF.

The class of extension $(**)$ is given by nonzero element $e(r^1,r^0)$ of the group

$$\begin{aligned}&\mathrm{Ext}_{\mathbb{F}_p[\Gamma]}(H^0,H^1)=\mathrm{H}^1(\Gamma,\mathrm{Hom}(H^0,H^1))=\\&=\mathrm{Hom}^{\Gamma_{\mathrm{tr}}}(I,\mathrm{Hom}(H^0,H^1))\subset\oplus_{\substack{\chi_1\in S(r^1)\\ \chi_0\in S(r^0)}}\mathrm{Hom}^{\Gamma_{\mathrm{tr}}}(I,\mathrm{Hom}(H^0_{\chi_0},H^1_{\chi_1}))\end{aligned}$$

(here I is the subgroup of higher ramification in Γ).

Conjugacy condition gives, if

$$e(r^1,r^0)_{\chi_0,\chi_1}\in\mathrm{Hom}^{\Gamma_{\mathrm{tr}}}(I,\mathrm{Hom}(H^0_{\chi_0},H^1_{\chi_1}))$$

is not trivial, then $e(r^1,r^0)_{\sigma\chi_0,\sigma\chi_1}$ also is not trivial (here σ is absolute Frobenius and $r(\sigma\chi_0)=r(\chi_0)(1), r(\sigma\chi_1)=r(\chi_1)(1)$).

3.11.2. For any $r\in R_p\setminus\{0\}=\{\ r\in\mathbb{Q}\cap(0,1]\mid v_p(r)\geq 0\ \}$ define the subfield $K(r)$ of K as follows. $K(r)$ is composite of fields

$$\{\ K_{\mathrm{tr}}(T_\beta)\mid\beta\in W(k)\ \},$$

where $T_\beta^p-T_\beta=\beta\theta_b^{-a}$, $r=a/b$, $a,b\in\mathbb{Z}$, $v_p(b)=0$ and $\theta_b\in K_{\mathrm{tr}}$ is such that $\theta_b^b=p$.

We have the following properties

a) $K(r)/K$ is Galois extension;

b) $I(r)=\mathrm{Gal}(K(r)/K_{\mathrm{tr}})$ is abelian group of exponent p;

c) $I(r)$ is isotypical $\mathbb{F}_p[\Gamma_{\mathrm{tr}}]$-module, where action of Γ_{tr} is given by the set of characters conjugated to the character χ, such that $r(\chi)=r$;

d) if $r = k/(p^{N_1}-1)$ for some $N_1 \in \mathbb{N}, k \in \mathbb{N}$, then $K(r)$ coincides with composite of fields from the set

$$\{\ K_{\mathrm{tr}}(T_{\beta,N_1}) \mid \beta \in W(k)\ \},$$

where $T_{\beta,N_1}^{p^{N_1}} - T_{\beta,N_1} = \beta\pi_{N_1}^{-k}$ and $\pi_{N_1}^{p^{N_1}-1} = -p$.

3.11.3. Use construction of modified Fontaine-Laffaille functor, c.f. the end of n.2.2. Elements of the Galois module $U_1(r^1, r^0)$ can be identified with residues modulo $p\bar{O}$ of solutions

$$\{\ (X_r \mid r \in S(r^0)\ ), (Y_r \mid r \in S(r^1)\ )\}$$

in $\bar{K}$ of the system of equations

$$\left(-\frac{1}{p}\right)^{l_0(r(-1))} X_{r(-1)}^p = X_r,\ \text{where } r \in S(r^0);$$

$$\left(-\frac{1}{p}\right)^{l_0(r(-1))} Y_{r(-1)}^p = Y_r + \sum_{(r',r)\in S_{(r^0,r^1)}} \beta_{rr'}^* X_{r'},$$

where $r \in S(r^1)$.

Over K_{tr} all solutions of this system can be expressed via solutions of equations

$$T^q - T = \beta_{rr'}^* \pi_N^{-k+k'},$$

where $q = p^N$, $\pi_N^{q-1} = -p$, $r = k/(q-1), r' = k'/(q-1)$.

Now the property d) of n.3.11.2 gives, that all points of $\mathbb{F}_p[\Gamma]$-module $U_1(r^1, r^0)$ are defined over composite of fields $K(r - r')$, where

$$(r', r) \in S_{(r^0,r^1)} = \{\ (r^0(i), r^1(i)) \mid i \in \mathbb{Z}\ \}.$$

3.11.4. Take $\chi_0 \in S(r^0), \chi_1 \in S(r^1)$, such that $e(r^1, r^0)_{\chi_0,\chi_1} \neq 0$. Then

$$e(r^1, r^0)_{\chi_0,\chi_1} \in \oplus_{(r',r)\in S_{(r^0,r^1)}} \mathrm{Hom}^{\Gamma_{\mathrm{tr}}}(I(r - r'), \mathrm{Hom}(H_{\chi_0}^0, H_{\chi_1}^1)).$$

There exists $(r_0', r_0) \in S_{(r^0,r^1)}$, such that the projection of $e(r^1, r^0)_{\chi_0,\chi_1}$ to

$$\mathrm{Hom}^{\Gamma_{\mathrm{tr}}}(I(-r + r'), \mathrm{Hom}(H_{\chi_0}^0, H_{\chi_1}^1))$$

is not trivial. Therefore, the character $\chi_0^{-1}\chi_1$ acts nontrivially on $I(r_0 - r_0')$ and for some $i \in \mathbb{Z}$ we have $r(\sigma^i(\chi_0^{-1}\chi_1)) = r_0 - r_0'$ (because $I(r_0 - r_0')$ is isotypical Γ_{tr}-module). This gives

$$-r(\chi_0)(i) + r(\chi_1)(i) \equiv r_0 - r_0' \bmod \mathbb{Z}.$$

Clearly, $(r_0', r_0) \in S_{(r^0,r^1)}$ implies $r_0 \neq r_0'$, and by the property C5 of the set S we have $r_0 = r(\chi_1)(i)$ and $r_0' = r(\chi_0)(i)$, i.e. $(r(\chi_0), r(\chi_1)) \in S_{(r^0,r^1)}$.

Therefore, by conjugacy condition the (χ^0, χ^1)-component $e(r^1, r^0)_{\chi^0, \chi^1}$ is also nontrivial.

Proposition and theorem A are proved.

3.12. *Remark.* Suppose the set S satisfies the condition C4 of n.1, i.e. $S = \{r, \dots, r(h-1)\}$, where $h = h(r)$. In this case $n_{\mathcal{U}(M)} = n_M$ takes values in $\mathbb{N} \cup \{+\infty\}$, and we can use its analogue

$$n_{\mathcal{U}(M),\chi} : \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}$$

from n.1.3 (where $\chi \in \operatorname{Char} \Gamma_{tr}$ is such that $r(\chi) = r$).

Consider the following property

C6. *The polynomes* $(l_0(r)X^{p^{h-1}} + \dots + l_{h-1}(r)X) \bmod p$ *and* $X^{p^h-1} - 1$ *are relatively prime in* $\mathbb{F}_p[X]$.

If our set S satisfies this additional assumption, we can prove, that $\mathcal{H}_0(\chi) = pW(\mathbb{F}_{p^h})e_{00}$, i.e. the second invariant of the image of the Galois group (c.f. n.1.3) takes maximal value.

Indeed, relate notation of n.1.3 with constructions of this section by taking $m = 1, r_1 = r, N = h_1 = h, M = M^*$ and $U = \mathcal{U}(M)$. We can take $e_0 = u_\chi^{(1)}$, then

$$m_r(e_0) \equiv u(0,1) \bmod p^2 A_{\text{cris}},$$

and for any $\tau \in \Gamma$

$$m_r(\tau e_0) \equiv w_{(1),\tau} u(0,1) \equiv m_r(w_{(1),\tau} e_0) \bmod p^2 A_{\text{cris}}.$$

By lemma of n.3.4

$$w_{(1),\tau} = \prod_{0 \le i < h} (\sigma^{-i} \eta_{LT}(\tau))^{l_i(r)}.$$

Now remark, that if τ runs over subgroup of higher ramification I of Γ, then its image in $\operatorname{Aut}_{\mathbb{Z}_p} U$ runs over pro-p-group H^1, $\eta_{LT}(\tau)$ runs over the subgroup of principal units of $W(\mathbb{F}_{p^h})$ and, therefore, $w_{(1),\tau} \bmod p^2 W(\mathbb{F}_{p^h})$ runs over the set

$$\mathcal{B}_r = \{\ 1 + p \sum_{0 \le i < h} (\sigma^{-i}\alpha) l_i(r) \bmod p^2 \mid \alpha \in \mathbb{F}_{p^h}\ \}.$$

This gives

$$\mathcal{H}_0(\chi) \bmod p^2 W(\mathbb{F}_{p^h}) e_{00} = \mathcal{B}_r e_{00}.$$

The correspondence

$$\alpha \mapsto \sum_{0 \le i < h} (\sigma^{-i}\alpha) l_i(r)$$

defines $\mathbb{F}_p$-linear morphism $b_r : \mathbb{F}_{p^h} \longrightarrow \mathbb{F}_{p^h}$. Clearly, assumption C6 implies, that $\operatorname{Ker} b_r = 0$ and, therefore, $\operatorname{Im} b_r = \mathbb{F}_{p^h}$. Therefore, $\mathcal{H}_0(\chi) \bmod p^2 W(\mathbb{F}_{p^h}) e_{00} = pW(\mathbb{F}_{p^h}) e_{00}$ and we obtain $\mathcal{H}_0(\chi) = pW(\mathbb{F}_{p^h}) e_{00}$.

References

[Ab1] V.A. Abrashkin, *Modification of the Fontaine-Laffaille functor*, Math. USSR Izvestiya **34** (1990), no. 3.

[Ab2] V.A. Abrashkin, *Modular representations of the Galois group of a local field, and a generalization of the Shafarevich conjecture*, Math. USSR Izvestiya **35** (1990), no. 3.

[Fo1] J.-M. Fontaine, *Points d'ordre fini d'un groupe formel sur une extension non ramifie de* $\mathbb{Z}_p$, Memoire 37, 1974, p. 75-79.

[Fo2] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Asterisque **47-48** (1977), Paris.

[F-L] J.-M. Fontaine, G. Laffaille, *Construction de representations p-adiques*, Ann. Sci. E.N.S. 4 serie **15** (1982), 547-608.

[Na] T. Nakamura, *On torsion points of formal groups over a ring of Witt vectors*, Math. Z. **193** (1986), 397-404.

[Wtb] J.-P. Wintenberger, *Un scindage de la filtration de Hodge pour certaines varietes algebriques sur le corps locaux*, Annals of Math. **119** (1984), 511-548.