Math-Net.Ru

Общероссийский математический портал

В. А. Абрашкин, Образ группы Галуа для некоторых кристаллических представлений, *Изв. РАН. Сер. матем.*, 1999, том 63, выпуск 1, 3–40

DOI: <https://doi.org/10.4213/im226>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.89.197.203

26 апреля 2023 г., 17:02:49

УДК 512.7

В. А. Абрашкин

Образ группы Галуа для некоторых кристаллических представлений

Пусть K – поле частных кольца векторов Витта $W(k)$, где k – алгебраически замкнутое поле характеристики $p > 0$, и $\Gamma = \text{Gal}(\overline{K}/K)$. Если U – Γ -инвариантная решетка в непрерывном $\mathbb{Q}_p[\Gamma]$ -модуле V конечной $\mathbb{Q}_p$ -размерности и множество характеров S полупростой оболочки $U \otimes \mathbb{F}_p$ удовлетворяет некоторым дополнительным условиям, то с U связывается функция $n_U: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$, которая содержит значительную часть информации об образе H_U группы Γ в $\text{Aut}_{\mathbb{Z}_p} U$. В работе получено описание функций, возникающих из кристаллических модулей V с весами Ходжа–Тейта из промежутка $[0, p-2]$, а также получено их явное выражение в терминах соответствующих фильтрованных модулей. Этот результат применяется к нахождению образа $H_{T(\mathcal{G})}$, где $T(\mathcal{G})$ – модуль Тейта 1-мерной формальной группы $\mathcal{G}$ над $W(k)$, имеющей конечную высоту.

Библиография: 9 наименований.

§ 0. Введение

Пусть K – поле частных кольца векторов Витта $W = W(k)$, где k – алгебраически замкнутое поле характеристики $p > 0$, и пусть $\Gamma = \text{Gal}(\overline{K}/K)$ – абсолютная группа Галуа поля K .

Для $a \in \mathbb{Z}$ такого, что $0 \leq a \leq p-1$, обозначим через $\text{MG}^{\text{cris}}(a)$ полную подкатегорию категории $\mathbb{Z}_p[\Gamma]$ -модулей, состоящую из Γ -инвариантных решеток кристаллических $\mathbb{Q}_p[\Gamma]$ -модулей с весами Ходжа–Тейта из промежутка $[0, a]$. Теория Фонтена–Лаффе (см. [7]) дает эффективный способ построения объектов категории $\text{MG}^{\text{cris}}(a)$ с помощью некоторого функтора (функтора Фонтена–Лаффе) $\mathcal{U}: \text{MF}_f(a) \rightarrow \text{MG}^{\text{cris}}(a)$, где $\text{MF}_f(a)$ – некоторая подкатегория категории фильтрованных W -модулей.

В предлагаемой работе мы следуем одной идее Ж.-М. Фонтена из [5] для изучения образа H группы Γ в $\text{Aut}_{\mathbb{Z}_p} U$, где $U \in \text{MG}^{\text{cris}}(a)$.

Пусть Γ_{tr} – группа Галуа максимального слабо разветвленного расширения K_{tr} поля K в $\overline{K}$. Фиксируем сечение $s: \Gamma_{\text{tr}} \rightarrow \Gamma$ естественной проекции $\Gamma \rightarrow \Gamma_{\text{tr}}$. Пусть U – свободный $\mathbb{Z}_p$ -модуль конечного ранга h с непрерывным действием группы Галуа Γ . С помощью сечения s мы можем рассматривать U как (полупростой) $\mathbb{Z}_p[\Gamma_{\text{tr}}]$ -модуль. Тогда $E = \text{End}_{\mathbb{Z}_p} U$ имеет естественную (зависящую от выбора сечения s) структуру $\mathbb{Z}_p[\Gamma_{\text{tr}}]$ -модуля. Рассмотрим следующие два основных предположения о структуре этих модулей (в действительности условие C2) влечет C1):

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 97-01-00934.

C1) в изотипическом разложении $U = \bigoplus_{\alpha \in \mathcal{J}} U_\alpha$ все компоненты U_α , $\alpha \in \mathcal{J}$, являются простыми;

C2) в изотипическом разложении $E = E^0 \oplus \left(\bigoplus_{\beta \in \mathcal{J}} E_\beta \right)$, где $E^0 = E^{s(\Gamma_{\text{tr}})}$, все компоненты (с нетривиальным действием группы Γ_{tr}) E_β , $\beta \in \mathcal{J}$, являются простыми.

Пусть $\overline{W} = W(\overline{\mathbb{F}}_p)$ и $\overline{U} = U \otimes \overline{W}$. Предположение C1) означает, что $\overline{U} = \bigoplus_{\chi \in S_U} U_\chi$, где S_U – конечное подмножество группы характеров $\text{Char } \Gamma_{\text{tr}}$, и для каждого $\chi \in S_U$ выполнено $\text{rk}_{\overline{W}} U_\chi = 1$. Множество S_U удовлетворяет условию сопряженности: $\chi \in S_U \Rightarrow \sigma\chi \in S_U$, где σ – абсолютный морфизм Фробениуса.

Для любого конечного σ -инвариантного подмножества $S \subset \text{Char } \Gamma_{\text{tr}}$ рассмотрим множество функций $\mathcal{F}_S$

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

таких, что для любых $\chi_1, \chi_2, \chi_3 \in S$ выполнены следующие свойства:

- a) $n(\chi_1, \chi_1) \geq 1$;
- b) $n(\chi_1, \chi_2) = n(\sigma\chi_1, \sigma\chi_2)$;
- c) $n(\chi_1, \chi_2) \leq n(\chi_1, \chi_3) + n(\chi_3, \chi_2)$;
- d) $n(\chi_1, \chi_1) = \min\{n(\chi_1, \chi) + n(\chi, \chi_1) \mid \chi \in S\}$.

Для исходного $\mathbb{Z}_p[\Gamma]$ -модуля U (если он как $\mathbb{Z}_p[\Gamma_{\text{tr}}]$ -модуль удовлетворяет предположениям C1) и C2)) функция $n_U \in \mathcal{F}_{S_U}$ может быть определена следующим образом.

Пусть G – образ подгруппы высшего ветвления $I = \text{Ker}(\Gamma \rightarrow \Gamma_{\text{tr}})$ в $\text{Aut}_{\mathbb{Z}_p} U \subset E$. Тогда G является замкнутой про- p -подгруппой в $\text{Aut}_{\mathbb{Z}_p} U$, и можно показать, что если $\tilde{G}$ – наименьшая замкнутая p -группа, содержащая G и “максимальный тор” $1 + pE^0$, то

$$\tilde{G} = \text{id}_U + pE^0 + \sum_{\beta \in \mathcal{J}} p^{n_\beta} E_\beta,$$

где для любого $\beta \in \mathcal{J}$ $n_\beta \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ (при $n_\beta = \infty$ мы считаем, что $p^{n_\beta} = 0$). Если $\chi_1, \chi_2 \in S$ таковы, что $\chi_1 \neq \chi_2$, то существует единственный индекс $\beta(\chi_1, \chi_2) \in \mathcal{J}$ такой, что характер $\chi_1^{-1}\chi_2$ появляется как характер Γ_{tr} -модуля $E_{\beta(\chi_1, \chi_2)}$, и мы полагаем

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

Если $\chi_1 = \chi_2$, то положим по определению

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

Определенная таким образом функция n_U принадлежит множеству $\mathcal{F}_{S_U}$ и несет в себе значительную часть информации об образе группы Γ в $\text{Aut}_{\mathbb{Z}_p} U$.

Можно проверить, что в описанной выше ситуации любая функция из множества $\mathcal{F}_S$ может быть реализована с помощью подходящего $\mathbb{Z}_p[\Gamma]$ -модуля U .

Пусть $a \in \mathbb{Z}_{\geq 0}$ таково, что $0 \leq a \leq p-1$, и пусть $(\text{Char } \Gamma_{\text{tr}})(a)$ – объединение всех S_U , где $U \in \text{MG}^{\text{cris}}(a)$. Обозначим через v_p p -адический показатель поля $\mathbb{Q}$ и рассмотрим стандартное отождествление

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

(напомним, что если $\chi \in \text{Char } \Gamma_{\text{tr}}$, то для некоторого натурального числа N выполнено равенство $r(\chi) = l/(p^N - 1)$, где $0 \leq l < p^N - 1$, $\chi = \chi_N^{*l}$ и $\chi_N^* \in \text{Char } \Gamma_{\text{tr}}$ таков, что $\chi_N^*(\tau) = (\tau\pi_N)\pi_N^{-1}$ для $\pi_N \in \bar{K}$, удовлетворяющего равенству $\pi_N^{p^N-1} = p$). Согласно теории Фонтена–Лаффе мы имеем

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

где $R_p(a)$ состоит из $r \in R'_p$ таких, что все цифры $l_s(r)$ p -ичного (архимедова) разложения

$$r = \frac{l_1(r)}{p} + \dots + \frac{l_s(r)}{p^s} + \dots$$

принадлежат промежутку $[0, a]$.

Пусть $a \leq p-2$. В этом случае функтор Фонтена–Лаффе $\mathcal{U}: \text{MF}_f(a) \rightarrow \text{MG}^{\text{cris}}(a)$ является антиэквивалентностью категорий. Если $U \in \text{MG}^{\text{cris}}(a)$, то $U = \mathcal{U}(M)$, где $M \in \text{MF}_f(a)$, и наш основной результат (теорема А из п. 2.5.1) дает явное выражение для функции n_U в терминах, относящихся к строению фильтрованного модуля M .

Пусть

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

Тогда (согласно теореме В из п. 2.5.2) подмножество $\mathcal{F}'_S \subset \mathcal{F}_S$ может быть охарактеризовано с помощью только одного дополнительного условия

d') если $\chi_1, \chi_0 \in S$, $r_1 = r(\chi_1)$, $r_0 = r(\chi_0)$ и для всех $s \in \mathbb{N}$ выполнено неравенство $l_s(r_0) \geq l_s(r_1)$, то

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

Если $\text{rk}_{\mathbb{Z}_p} U = h$ и образ группы Γ_{tr} в $\text{Aut}_{\mathbb{Z}_p} U$ имеет порядок $p^h - 1$, то (см. § 1) U удовлетворяет предположениям C1) и C2), S_U состоит из одной σ -орбиты. В этом случае условие d') сводится к условию d) и, следовательно, $\mathcal{F}'_{S_U} = \mathcal{F}_{S_U}$. В частности, эти соображения применимы, если $a = 1$, $p \geq 3$, а U – модуль Тейта 1-мерной формальной группы над W , и мы получаем положительный ответ на вопрос Ж.-М. Фонтена из [5]. В этом случае функция n_U может быть также выражена в терминах функционального уравнения для логарифма соответствующей формальной группы (см. § 2).

Мы не рассматриваем в этой работе случай $a = p-1$, но он может быть рассмотрен аналогичным образом, если заменить функтор Фонтена–Лаффе на его некоторую модификацию (на уровне объектов, аннулируемых умножением на p , эта модификация была построена в работе [1]).

Как будет отмечено в § 1, знание функции n_U эквивалентно знанию образа H группы Галуа в $\text{Aut}_{\mathbb{Z}_p} U$, если “максимальный тор” $\text{id}_U + pE^0$ лежит в H . В § 3 мы приводим одно достаточное условие для этого свойства максимального тора и применяем его к случаю Γ -модулей, возникающих из модулей Тейта формальных групп над кольцом W .

§ 1. Описание некоторых подгрупп группы $\text{GL}_h(\mathbb{Z}_p)$

Обозначим через U свободный $\mathbb{Z}_p$ -модуль конечного ранга h , снабженный естественным действием циклической подгруппы $H_1 \subset \text{Aut}_{\mathbb{Z}_p} U \simeq \text{GL}_h(\mathbb{Z}_p)$. Мы предполагаем, что порядок группы H_1 взаимно прост с p . Обозначим через $\overline{W}$ кольцо векторов Витта с коэффициентами из $\overline{\mathbb{F}}_p$ и положим $\overline{U} = U \otimes_{\mathbb{Z}_p} \overline{W}$.

1.1. Пусть S_U – множество характеров χ группы H_1 со значениями в $\overline{W}^*$ таких, что

$$U_\chi = \{u \in \overline{U} \mid hu = \chi(h)u \text{ и } \forall h \in H_1\} \neq 0.$$

Очевидно, если σ – абсолютный морфизм Фробениуса на $\overline{W}$, то множество S_U инвариантно относительно естественного действия σ . Пусть $\mathcal{J}$ – множество орбит морфизма σ на множестве S_U . Тогда

$$U = \bigoplus_{\alpha \in \mathcal{J}} U_\alpha, \quad U_\alpha \otimes \overline{W} = \bigoplus_{\chi \in S_{U,\alpha}} U_\chi, \quad S_U = \coprod_{\alpha \in \mathcal{J}} S_{U,\alpha}.$$

Если $\chi \in S_U$, то $\alpha(\chi) \in \mathcal{J}$ будет обозначать единственный индекс такой, что $\chi \in S_{U,\alpha(\chi)}$.

Рассмотрим следующее свойство $\mathbb{Z}_p[H_1]$ -модуля U .

C1. $\text{rk}_{\overline{W}} U_\chi = 1$ для любого $\chi \in S_U$, т.е. $\mathbb{Z}_p[H_1]$ -модуль U не содержит кратных неприводимых компонент.

Рассмотрим множество $E = \text{End}_{\mathbb{Z}_p} U$ с естественной структурой $\mathbb{Z}_p[H_1]$ -модуля (возникающей из действия H_1 на U). Пусть S_E – множество характеров группы H_1 со значениями в $\overline{W}^*$ такое, что

$$\overline{E} := E \otimes \overline{W} = \bigoplus_{\chi \in S_E} E_\chi$$

и $E_\chi \neq 0$ для любого $\chi \in S_E$. Тогда $S_E = \{\chi_1^{-1}\chi_2 \mid \chi_1, \chi_2 \in S_U\}$. Обозначим через 1_{H_1} тривиальный характер группы H_1 и положим $S'_E = S_E \setminus \{1_{H_1}\}$. Множество S'_E инвариантно относительно σ , и можно рассмотреть его разложение в объединение непересекающихся σ -орбит $S'_E = \coprod_{\beta \in \mathcal{J}} S'_{E,\beta}$. Для произвольных $\chi_1, \chi_2 \in S_U$ таких, что $\chi_1 \neq \chi_2$, мы будем использовать обозначение $\beta(\chi_1, \chi_2)$ для единственного индекса $\beta \in \mathcal{J}$ такого, что $\chi_1^{-1}\chi_2 \in S'_{E,\beta}$.

Пусть $E^0 = (\text{End}_{\mathbb{Z}_p} U)^{H_1}$; тогда имеется разложение $\mathbb{Z}_p[H_1]$ -модулей

$$E = E^0 \oplus \left(\bigoplus_{\beta \in \mathcal{J}} E_\beta \right),$$

где

$$E^0 \otimes \overline{W} = \bigoplus_{\chi \in S_U} \text{End}_{\overline{W}}(U_\chi, U_\chi), \quad E_\beta \otimes \overline{W} = \bigoplus_{\beta(\chi_1, \chi_2) = \beta} \text{Hom}_{\overline{W}}(U_{\chi_1}, U_{\chi_2})$$

по отношению к разложению

$$\overline{E} = \text{End}_{\overline{W}}(\overline{U}) = \bigoplus_{\chi_1, \chi_2 \in S_U} \text{Hom}(U_{\chi_1}, U_{\chi_2}).$$

Рассмотрим следующее свойство $\mathbb{Z}_p[H_1]$ -модуля E .

C2. Если $\chi_1, \chi_2, \chi_3, \chi_4 \in S_U$, $\chi_1 \neq \chi_2$ и $\chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$, то $\chi_1 = \chi_3$ (и, следовательно, $\chi_2 = \chi_4$), т.е. $\mathbb{Z}_p[H_1]$ -модуль $\text{End}_{\mathbb{Z}_p} U$ не содержит неприводимой кратной компоненты с нетривиальным действием H_1 .

Отметим, что из свойства C2 вытекает свойство C1.

Для иллюстрации этих свойств докажем следующее предложение.

ПРЕДЛОЖЕНИЕ. Если H_1 — циклическая группа порядка $q - 1$, где $q = p^h$, то свойства C1 и C2 выполнены и U является простым $\mathbb{Z}_p[H_1]$ -модулем.

ДОКАЗАТЕЛЬСТВО. Для произвольного $\alpha \in \mathcal{J}$ выберем характер $\chi_\alpha \in S_{U, \alpha}$ и обозначим через $h_\alpha \in \mathbb{N}$ минимальное натуральное число такое, что $S_{U, \alpha} = \{\chi_\alpha, \dots, \sigma^{h_\alpha-1}\chi_\alpha\}$. Тогда для $\alpha \in \mathcal{J}$ мы получаем, что $\text{ord } \chi_\alpha \mid (p^{h_\alpha} - 1)$ и $\sum_{\alpha \in \mathcal{J}} h_\alpha = |S_U| \leq h$. Теперь

$$q - 1 = \text{НОК}\{\text{ord } \chi_\alpha \mid \alpha \in \mathcal{J}\} \leq \prod_{\alpha \in \mathcal{J}} (p^{h_\alpha} - 1) \leq p^{|S_U|} - |\mathcal{J}|$$

влечет $|\mathcal{J}| = 1$ и $|S_U| = h$. Другими словами, существует характер χ такой, что $S_U = \{\chi, \sigma\chi, \dots, \sigma^{h-1}\chi\}$ и $\text{ord } \chi = q - 1$. Таким образом, свойство C1 выполнено.

Пусть $\chi_1, \dots, \chi_4 \in S_U$, $\chi_1 \neq \chi_2$ и $\chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$. Мы можем считать, что $\chi_1 = \chi$, $\chi_2 = \sigma^{n_2}\chi$, $\chi_3 = \sigma^{n_3}\chi$ и $\chi_4 = \sigma^{n_4}\chi$, где $0 \leq n_2, n_3, n_4 < h$ и $n_2 \neq 0$. Так как $\text{ord } \chi = q - 1$, равенство $\chi_1^{-1}\chi_2 = \chi_3^{-1}\chi_4$ может быть переписано в виде сравнения

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

Обе части этого сравнения принимают значения из отрезка $[2, q]$, поэтому мы получаем равенство $1 + p^{n_4} = p^{n_2} + p^{n_3}$. Теперь $n_2 \neq 0 \Rightarrow 1 + p^{n_4} \geq p + 1 > 2 \Rightarrow n_4 \neq 0 \Rightarrow n_3 = 0 \Rightarrow \chi_1 = \chi_3$. Таким образом, свойство C2 также выполнено.

1.2. Обозначим через Gr_U множество всех замкнутых (в p -адической топологии) про- p -подгрупп G в $\text{Aut}_{\mathbb{Z}_p} U \subset E$ таких, что $h^{-1}Gh = G$ для любого $h \in H_1$. Впредь мы будем предполагать, что U удовлетворяет условиям C1, C2 из п. 1.1.

Типичный элемент множества Gr_U может быть построен следующим образом. В использованных выше обозначениях положим $S = S_U$ и обозначим через $\mathcal{F}_S$ множество функций

$$n: (\chi_1, \chi_2) \mapsto n(\chi_1, \chi_2) \in \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

удовлетворяющих следующим условиям, где $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$:

- а) $n(\sigma\chi_1, \sigma\chi_2) = n(\chi_1, \chi_2)$;
- б) $n(\chi_1, \chi_2) + n(\chi_2, \chi_1) \geq 1$;
- в) $n(\chi_1, \chi_3) + n(\chi_3, \chi_2) \geq n(\chi_1, \chi_2)$, если $\chi_3 \in S$ и $\chi_3 \neq \chi_1, \chi_2$.

Если $\beta \in \mathcal{J}$, то положим $n_\beta = n(\chi_1, \chi_2)$, где $\beta = \beta(\chi_1, \chi_2)$. Если $n \in \mathcal{F}_S$, то положим

$$G[n] := \text{id}_U + pE^0 + \sum_{\beta \in \mathcal{J}} p^{n_\beta} E_\beta.$$

Следующая лемма является очевидной.

ЛЕММА 1. $G[n] \in \text{Gr}_U$.

Для любых $n \in \mathcal{F}_S$ и $\chi \in S$ положим временно $n(\chi, \chi) = 1$ и определим для произвольных $\chi_1, \chi_2 \in S$ таких, что $\chi_1 \neq \chi_2$,

$$n'(\chi_1, \chi_2) = \min\{n(\chi_1, \chi) + n(\chi, \chi_2) \mid \chi \in S\}.$$

Легко проверить, что $n' \in \mathcal{F}_S$. Как и ранее, положим для произвольного $\beta \in \mathcal{J}$ $n'_\beta = n'(\chi_1, \chi_2)$, если $\beta = \beta(\chi_1, \chi_2)$.

Следующая лемма доказывается непосредственными вычислениями.

ЛЕММА 2. $\text{id}_U + p^2 E^0 + \sum_{\beta \in \mathcal{J}} p^{n'_\beta} E_\beta \subset G[n]^p(G[n], G[n]) \subset G[n']$.

Заметим, что существует естественный изоморфизм $\mathbb{F}_p[H_1]$ -модулей

$$G[n]/G[n]^p(G[n], G[n]) \simeq \bigoplus_{\beta \in \mathcal{J}, n_\beta \neq n'_\beta} (E_\beta \otimes \mathbb{F}_p) \oplus A,$$

где A – конечная абелева группа периода p с тривиальным действием H_1 .

1.3. Пусть $G \in \text{Gr}_U$. Рассматривая G как подмножество в $\text{End}_{\mathbb{Z}_p} U = E^0 \oplus \left(\bigoplus_{\beta \in \mathcal{J}} E_\beta \right)$, положим

$$n_{G,\beta} = \min\{v_p(\text{pr}_{E_\beta}(\tau)) \mid \tau \in G\}$$

и $n_G(\chi_1, \chi_2) = n_{G,\beta}$, если $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$ и $\beta = \beta(\chi_1, \chi_2)$.

Обозначим через $\tilde{G}$ минимальную подгруппу в $\text{Aut}_{\mathbb{Z}_p} U$, которая содержит G и “максимальный тор” $1 + pE^0$.

ПРЕДЛОЖЕНИЕ. Во введенных выше обозначениях мы имеем:

- а) $n_G \in \mathcal{F}_S$;
- б) $\tilde{G} = G[n_G]$.

ДОКАЗАТЕЛЬСТВО. Отметим сначала, что функция n_G удовлетворяет свойствам а) и б) из определения элементов множества $\mathcal{F}_S$. Положим для произвольных $\chi_1, \chi_2 \in S$ таких, что $\chi_1 \neq \chi_2$,

$$n(\chi_1, \chi_2) = \min \{ n_G(\chi_1, \chi^{(1)}) + \dots \\ \dots + n_G(\chi^{(l-1)}, \chi^{(l)}) + n_G(\chi^{(l)}, \chi_2) \mid l \geq 0, \chi^{(1)}, \dots, \chi^{(l)} \in S \}.$$

Легко видеть, что эта функция n удовлетворяет следующим свойствам:

- 1) $n \in \mathcal{F}_S$;
- 2) для любых $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$, выполнено $n_G(\chi_1, \chi_2) \geq n(\chi_1, \chi_2)$;
- 3) $n_G \in \mathcal{F}_S$ тогда и только тогда, когда $n = n_G$.

Заметим, что из свойства 2) вытекает, что $G \subset G[n]$ и, следовательно, $\tilde{G} \subset G[n]$. Определим, как и в п. 1.2, функцию $n' \in \mathcal{F}_S$. Следующая лемма легко вытекает из определений.

ЛЕММА 1. Если $\chi_1, \chi_2 \in S$, $\chi_1 \neq \chi_2$, то либо $n'(\chi_1, \chi_2) = n(\chi_1, \chi_2)$, либо $n'(\chi_1, \chi_2) - 1 = n(\chi_1, \chi_2) = n_G(\chi_1, \chi_2)$.

Из этой леммы следует, что вложение $\tilde{G} \subset G[n]$ индуцирует сюръективный гомоморфизм $\tilde{G} \rightarrow G[n]/G[n]^p(G[n], G[n])$. Следовательно, $\tilde{G} = G[n]$ и, в частности, $n_{\tilde{G}} = n$.

Осталось только доказать, что $n_G = n_{\tilde{G}}$. Рассмотрим ряд Жордана–Гельдера для операторной H_1 -группы $\tilde{G}$

$$\tilde{G} = \tilde{G}_0 \supset \tilde{G}_1 \supset \dots \supset \tilde{G}_s \supset \dots$$

Легко видеть, что

$$G = G_0 \supset G_1 \supset \dots \supset G_s \supset \dots,$$

где $G_s = \tilde{G}_s \cap G$ для всех $s \geq 0$, является рядом Жордана–Гельдера для операторной H_1 -группы G . Теперь равенство $n_G = n_{\tilde{G}}$ вытекает из следующей леммы (мы опускаем ее доказательство).

ЛЕММА 2. Если $\beta \in \mathcal{J}$ и для некоторого $s \in \mathbb{Z}_{\geq 0}$ операторная H_1 -группа $\bar{E}_\beta = E_\beta \otimes \mathbb{F}_p$ содержится в факторе $\tilde{G}_s/\tilde{G}_{s+1}$, то $\bar{E}_\beta$ содержится также в факторе G_s/G_{s+1} .

1.4. Предположим, что $n \in \mathcal{F}_S$. Тогда эта функция может быть доопределена до функции, определенной для всех пар $(\chi_1, \chi_2) \in S \times S$ с помощью равенства

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

В результате множество функций $\mathcal{F}_S$ отождествляется с множеством функций

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

таких, что для всех $\chi_1, \chi_2, \chi_3 \in S$ выполнены следующие четыре свойства:

- $\mathcal{F}_1$) $n(\chi_1, \chi_1) \geq 1$;
- $\mathcal{F}_2$) $n(\sigma\chi_1, \sigma\chi_2) = n(\chi_1, \chi_2)$;
- $\mathcal{F}_3$) $n(\chi_1, \chi_3) + n(\chi_3, \chi_2) \geq n(\chi_1, \chi_2)$;
- $\mathcal{F}_4$) $n(\chi_1, \chi_1) = \min \{ n(\chi_1, \chi) + n(\chi, \chi_1) \mid \chi \in S \}$;

и предложение п. 1.3 дает следующее утверждение.

ПРЕДЛОЖЕНИЕ. Соответствие $\pi: n \mapsto G[n]$ задает инъективное отображение

$$\pi: \mathcal{F}_{S_U} \longrightarrow \mathrm{Gr}_U,$$

образ которого состоит из всех $G \in \mathrm{Gr}_U$, которые содержат “максимальный тор” $1 + pE^0$.

Предположим дополнительно, что U удовлетворяет следующему условию:

СЗ. U – простой $\mathbb{Z}_p[H_1]$ -модуль.

Если мы фиксируем характер $\chi \in S_U$, то $S_U = \{\chi, \dots, \sigma^{h-1}\chi\}$. Легко видеть, что если $n \in \mathcal{F}_{S_U}$, то $n(\chi_1, \chi_2) \geq 1$ для всех $\chi_1, \chi_2 \in S_U$.

Для $i \in \mathbb{Z}/h\mathbb{Z}$ положим

$$n_\chi(i) = n(\sigma^{m_1}\chi, \sigma^{m_2}\chi_2),$$

где $(m_2 - m_1) \bmod h = i$. Соответствие $n \mapsto n_\chi$ определяет отождествление (которое зависит от сделанного выше выбора характера $\chi \in S_U$) множества $\mathcal{F}_{S_U}$ с множеством всех функций

$$n: \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{\infty\}$$

таких, что

$$\begin{aligned} n(0) &= \min\{n(i) + n(-i) \mid i \in \mathbb{Z}/h\mathbb{Z}\}, \\ n(i+j) &\leq n(i) + n(j) \quad \forall i, j \in \mathbb{Z}/h\mathbb{Z}. \end{aligned}$$

§ 2. Случай модулей Фонтена–Лаффе

Пусть $W = W(k)$ – кольцо векторов Витта с коэффициентами в совершенном поле k характеристики $p > 0$. Пусть K – поле частных кольца W и $\Gamma = \mathrm{Gal}(\bar{K}/K)$. Пусть U – свободный $\mathbb{Z}_p$ -модуль конечного ранга h с непрерывным действием группы Γ . С арифметической точки зрения наиболее интересен случай, когда U является Γ -инвариантной решеткой некоторого кристаллического $\mathbb{Q}_p[\Gamma]$ -модуля. Условие кристалличности связано лишь с действием подгруппы инерции группы Γ , поэтому можно считать, что поле вычетов k является алгебраически замкнутым. Мы также ограничимся случаем кристаллических модулей с весами Ходжа–Тейта из промежутка $[0, a]$, где $a \in \mathbb{Z}$, $0 \leq a < p$, так как в этом случае применима теория Фонтена–Лаффе (фактически мы изучим случай, когда $a \leq p - 2$). Такие Γ -модули U мы будем для краткости называть Γ -модулями Фонтена–Лаффе.

Рассмотрим точную последовательность проконечных групп

$$1 \longrightarrow I \longrightarrow \Gamma \longrightarrow \Gamma_{\mathrm{tr}} \longrightarrow 1,$$

где Γ_{tr} – группа Галуа максимального слабо разветвленного расширения поля K , I – подгруппа высшего ветвления. Хорошо известно, что I – про- p -группа, Γ_{tr} – свободная проциклическая группа (обобщенного) порядка, взаимно простого с p , так

как поле вычетов k предполагается алгебраически замкнутым. Следовательно, существует сечение $s: \Gamma_{\text{tr}} \rightarrow \Gamma$ естественной проекции Γ на Γ_{tr} , и Γ отождествляется с полупрямым произведением Γ_{tr} и I . Пусть гомоморфизм $\rho: \Gamma \rightarrow \text{Aut}_{\mathbb{Z}_p} U$ отвечает структуре Γ -модуля на U . Положим $H = \rho(\Gamma)$, $H_1 = \rho(s(\Gamma_{\text{tr}}))$ и $G = \rho(I)$. Тогда H_1 – циклическая группа порядка, взаимно простого с p , G – замкнутая (в p -адической топологии) про- p -группа в $\text{Aut}_{\mathbb{Z}_p} U$, причем для любого $h \in H_1$ выполнено $h^{-1}Gh = G$ (т.е. $G \in \text{Gr}_U$ в обозначениях §1), и H является полупрямым произведением H_1 и G . Таким образом, мы можем использовать рассуждения из §1 для описания структуры группы H . Имея в виду исходную структуру Γ -модуля U , мы будем использовать обозначение n_U вместо обозначения n_G из §1. Отметим также, что при этих соглашениях условия C1) и C2) из введения согласованы с обозначенными теми же символами условиями из §1.

2.1. Некоторые факты из теории Фонтена–Лаффе [7]. Пусть A_{cris} – кристаллическое кольцо Фонтена. Оно снабжено непрерывным Γ -действием, причем $A_{\text{cris}}^{\Gamma} = W$. На нем также имеется эндоморфизм Фробениуса σ , который продолжает обычный морфизм Фробениуса кольца векторов Витта W . Кольцо A_{cris} имеет убывающую фильтрацию идеалов $\text{Fil}^i A_{\text{cris}}$, причем $\sigma \text{Fil}^i A_{\text{cris}} \subset p^i A_{\text{cris}}$ при $0 \leq i < p$.

Пусть $\mathcal{MF}$ – категория W -модулей M с убывающей фильтрацией длины $< p$ посредством W -подмодулей $M = M^0 \supset M^1 \supset \dots \supset M^p = 0$ и σ -линейными морфизмами $\phi_i: M^i \rightarrow M$ такими, что $\phi_i|_{M^{i+1}} = p\phi_{i+1}$ для всех $0 \leq i < p$.

Можно рассматривать A_{cris} также как объект категории $\mathcal{MF}$, если $A_{\text{cris}}^i = \text{Fil}^i A_{\text{cris}}$, $\phi_i = p^{-i}\sigma$ для $0 \leq i < p$ и $A_{\text{cris}}^p = 0$.

Пусть MF – полная подкатегория допустимых модулей в категории $\mathcal{MF}$. По определению MF состоит из конечно порожденных фильтрованных модулей $M \in \mathcal{MF}$ таких, что $\sum_i \phi_i(M^i) = M$. Категория MF является абелевой категорией. Обозначим через MF_f (соответственно через MF_{tor}) полную подкатегорию в категории MF , состоящую из свободных (соответственно периодических) W -модулей M . Для $a \in \mathbb{Z}_{\geq 0}$ такого, что $0 \leq a < p$, мы используем обозначения $\text{MF}(a)$, $\text{MF}_f(a)$ и $\text{MF}_{\text{tor}}(a)$ для полных подкатегорий соответственно в категориях MF , MF_f и MF_{tor} , состоящих из фильтрованных модулей M таких, что $M^{a+1} = 0$.

Пусть MG – категория $\mathbb{Z}_p[\Gamma]$ -модулей. Тогда теория Фонтена–Лаффе дает точный строгий функтор $\mathcal{U}: \text{MF} \rightarrow \text{MG}$. Если $M \in \text{MF}_f$, то $\mathcal{U}(M) = \text{Hom}_{\mathcal{MF}}(M, A_{\text{cris}})$, где структура Γ -модуля на $\mathcal{U}(M)$ индуцирована структурой Γ -модуля на A_{cris} . В этом случае $\mathcal{U}(M)$ является свободным $\mathbb{Z}_p$ -модулем, $\text{rk}_{\mathbb{Z}_p} \mathcal{U}(M) = \text{rk}_W M$ и $\mathcal{U}(M) \otimes \mathbb{Q}_p$ – кристаллический $\mathbb{Q}_p[\Gamma]$ -модуль с весами из промежутка $[0, a]$, если $M \in \text{MF}_f(a)$. Если $M \in \text{MF}_{\text{tor}}$, то

$$\mathcal{U}(M) = \text{Hom}_{\mathcal{MF}}(M, A_{\text{cris}, \infty}),$$

где $A_{\text{cris}, \infty} = \varinjlim_{n \in \mathbb{N}} A_{\text{cris}, n}$, и $A_{\text{cris}, n} = A_{\text{cris}}/p^n A_{\text{cris}}$ с индуцированной структурой объекта категории $\mathcal{MF}$. В этом случае длины W -модуля M и $\mathbb{Z}_p$ -модуля $\mathcal{U}(M)$ совпадают.

Первая информация о Γ -модулях $\mathcal{U}(M)$, где $M \in \text{MF}$, получается из изучения простых объектов категории MF . Пусть $R_p = \{r \in \mathbb{Q} \cap [0, 1] \mid v_p(r) \geq 0\}$, где v_p – p -адический показатель поля $\mathbb{Q}$.

Для любого $r \in R_p$ рассмотрим его p -ичное (архимедово) разложение

$$r = \frac{l_1(r)}{p} + \dots + \frac{l_s(r)}{p^s} + \dots$$

с цифрами $l_s(r)$, где $0 \leq l_s(r) < p$ при всех $s \in \mathbb{N}$. Обозначим через $h(r)$ минимальный положительный период последовательности $\{l_s(r)\}_{s \geq 1}$. Мы можем использовать индексы из $\mathbb{Z}/h(r)\mathbb{Z}$ или из $\mathbb{Z}$ для указания элементов этой последовательности.

Пусть $r \in R_p$ и $M(r) \in \text{MF}$ таков, что:

- а) $pM(r) = 0$ и как k -модуль $M(r)$ имеет базис $\{m_i \mid i \in \mathbb{Z}/h(r)\mathbb{Z}\}$;
- б) для $0 \leq j < p$ подмодуль фильтрации $M(r)^j$ порожден элементами множества

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

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

- с) для всех $i \in \mathbb{Z}/h(r)\mathbb{Z}$ имеем $\phi_{l_i(r)}(m_i) = m_{i+1}$.

Если $r \in R_p$ и $i \in \mathbb{Z}$, пусть

$$r(i) = \frac{l_{i+1}(r)}{p} + \dots + \frac{l_{i+s}(r)}{p^s} + \dots$$

Тогда произвольный простой объект категории MF изоморфен $M(r)$ для некоторого $r \in R_p$, и $M(r_1) \simeq M(r)$, если и только если $r_1 = r(i)$ для некоторого $i \in \mathbb{Z}$.

Для $N \in \mathbb{N}$ определим “слабо разветвленный” характер $\chi_N^*: \Gamma \rightarrow W^*$ с помощью соотношения

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

где $\tau \in \Gamma$ и $\pi_N \in \overline{K}$ таков, что $\pi_N^{p^N-1} = p$. Если $\chi: \Gamma \rightarrow W^*$ – непрерывный характер, то $\chi = \chi_N^{*k_N(\chi)}$ для некоторых $N \in \mathbb{N}$ и $0 \leq k_N(\chi) < p^N - 1$. В этих обозначениях рациональное число

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

не зависит от выбора натурального числа N и определяет характер χ однозначно. Этот инвариант может быть использован для описания структуры Γ -модуля $U(r) = \mathcal{U}(M(r))$. Если $r \in R'_p$, то $U(r)$ является простым $\mathbb{Z}_p[\Gamma]$ -модулем с множеством характеров $S = \{\chi, \sigma\chi, \dots, \sigma^{h(r)-1}\chi\}$, где $r(\chi) = r$. Это означает, что $pU(r) = 0$ и

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

где $U(r)_\eta = \{u \in U(r) \otimes W \mid \tau u = \eta(\tau)u \text{ для всех } \tau \in \Gamma\} \neq 0$. Если $r = 1$, то $U(1) = U(0)$ – тривиальный Γ -модуль $\mathbb{F}_p$.

Пусть V – кристаллический $\mathbb{Q}_p[\Gamma]$ -модуль с весами из промежутка $[0, a]$, где $0 \leq a \leq p - 2$. Если $U \subset V$ является Γ -модулем Фонтена–Лаффе, то существует $M \in \text{MF}_f(a)$ такой, что $U = \mathcal{U}(M)$, так как ограничение функтора Фонтена–Лаффе на подкатегорию $\text{MF}(p-2)$ является вполне строгим. Объекты M подкатегории $\text{MF}(a)$ могут быть охарактеризованы следующим образом: $M \in \text{MF}(a)$

тогда и только тогда, когда $M \in \text{MF}$, и если $M(r)$ – простой подфактор в M , то $r \in R_p(a)$, где $R_p(a) = \{r \in R_p \mid 0 \leq l_s(r) \leq a \text{ для всех } s \in \mathbb{N}\}$.

Ниже нам понадобится следующее явное описание ограничения $\mathcal{U}_1$ функтора $\mathcal{U}$ на подкатегорию $\text{MF}_1(p-2)$, состоящую из модулей $M \in \text{MF}(p-2)$, аннулируемых умножением на p .

Пусть $M \in \text{MF}_1(p-2)$; тогда он имеет k -базис $\bar{m} = (m_1, \dots, m_N)$ такой, что для некоторой функции $l: [1, N] \rightarrow [0, p-2]$ подмодуль фильтрации M^j , где $0 \leq j \leq p-2$, порожден элементами множества $\{m_i \mid l(i) \geq j\}$. Если $\bar{\phi}(\bar{m}) = (\phi_{l(1)}(m_1), \dots, \phi_{l(N)}(m_N))$, то σ -линейные морфизмы $\phi_j: M^j \rightarrow M$, где $0 \leq j \leq p-2$, однозначно определены соотношением

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

для некоторой матрицы $C \in \text{GL}_N(W(k))$. Тогда $\mathcal{U}_1(M)$ может быть отождествлен с Γ -модулем вычетов по модулю $p\bar{O}$ всех $\bar{K}$ -решений $\bar{X} = (X_1, \dots, X_N)$ системы уравнений

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

ЗАМЕЧАНИЕ. На всей категории $\text{MF} = \text{MF}(p-1)$ функтор Фонтена–Лаффе уже не является вполне строгим, но изложенная выше конструкция функтора $\mathcal{U}_1 = \mathcal{U}|_{\text{MF}_1(p-2)}$ все еще имеет смысл для объектов категории MF_1 – полной подкатегории в MF_{tor} , состоящей из фильтрованных модулей M таких, что $pM = 0$, и дает достаточно хорошую модификацию функтора Фонтена–Лаффе, определенную на всей категории MF (см. [1]). При необходимости эта модификация может быть использована для распространения основных результатов этой работы на случай модулей Фонтена–Лаффе с весами из промежутка $[0, p-1]$.

2.2. Класс $\text{MF}^{(S)}$. Пусть S – конечное подмножество в R_p такое, что $r \in S \Rightarrow r(1) \in S$. Для любого $r \in S$ рассмотрим его p -ичное разложение

$$r = \frac{l_1(r)}{p} + \dots + \frac{l_s(r)}{p^s} + \dots,$$

где $0 \leq l_s(r) < p$ для всех $s \in \mathbb{N}$.

Введем класс $\text{MF}^{(S)}$ объектов категории MF_f следующим образом. По определению этот класс состоит из фильтрованных свободных W -модулей M таких, что:

- а) M имеет W -базис $\{m_r \mid r \in S\}$ и для любого $0 \leq j \leq p$ соответствующий подмодуль фильтрации M^j порожден элементами множества $\{m_r \mid l_0(r) \geq j\}$ (в частности, для любого $r \in S$ выполнено $m_r \in M^{l_0(r)} \setminus M^{l_0(r)+1}$);
- б) σ -линейные морфизмы $\phi_j: M^j \rightarrow M$ однозначно определены соотношениями

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

где $r \in S$, а коэффициенты $\beta_{rr'} \in W$ удовлетворяют следующим условиям:

b₁) пусть $r_1, \dots, r_m \in S$ таковы, что

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

где $h_j = h(r_j)$ – минимальный период p -ичного разложения для $r_j \in S$; тогда существует подстановка $\begin{pmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{pmatrix}$ такая, что

если $r = r_{j_a}(\alpha)$ и $r' = r_{j_b}(\beta)$, где $a \geq b$, $\alpha \in \mathbb{Z}/h_{j_a}\mathbb{Z}$ и $\beta \in \mathbb{Z}/h_{j_b}\mathbb{Z}$, то $\beta_{rr'} \in pW$;

b₂) если $l_0(r) \leq l_0(r')$, то $\beta_{rr'} = 0$.

Приведенные выше условия а) и b₁) определяют на M структуру объекта категории MF_f , а условие b₁) описывает $M/pM = M^{(1)} \in \text{MF}_{\text{tor}}$ в виде последовательных расширений простого объекта $M(r_{j_1})$ с помощью простых объектов $M(r_{j_a})$, где $1 < a \leq m$. Другими словами, имеются следующие точные последовательности в категории MF_{tor} :

$$\begin{aligned} 0 \longrightarrow M^{(2)} \longrightarrow M^{(1)} \longrightarrow M(r_{j_1}) \longrightarrow 0, \\ \dots\dots\dots \\ 0 \longrightarrow M(r_{j_m}) = M^{(m)} \longrightarrow M^{(m-1)} \longrightarrow M(r_{j_{m-1}}) \longrightarrow 0. \end{aligned}$$

ЗАМЕЧАНИЕ. Условие b₂) было введено Ж.-П. Винтенберже (см. [9]). Он доказал, что структура произвольного $M \in \text{MF}_f$ может быть задана с помощью удовлетворяющего этому свойству аналога описанной выше явной конструкции (что также дает функториальное расщепление соответствующей фильтрации на M).

Очевидно, $\text{MF}^{(S)} \subset \text{MF}(p-2)$, если и только если $S \subset R_p(p-2)$. Если $M \in \text{MF}^{(S)}$ и $U = \mathcal{U}(M)$, то множество S_U характеров соответствующего Γ_{tr} -модуля (см. п. 1.1) отождествляется с S с помощью соответствия $\chi \mapsto r(\chi)$ (см. п. 2.1 по поводу определения инварианта $r(\chi)$). Очевидно, U удовлетворяет свойству C1 из § 1. Таким образом, мы получили следующее предложение.

ПРЕДЛОЖЕНИЕ. Следующие свойства модуля Галуа U эквивалентны:

- 1) U – модуль Фонтена–Лаффе с весами из промежутка $[0, p-2]$, удовлетворяющий условию C1 из § 1;
- 2) $U \simeq \mathcal{U}(M)$, где $M \in \text{MF}^{(S)}$ и $S \subset R_p(p-2)$.

Рассмотрим следующее свойство подмножества $S \subset R_p(p-2)$:

C4. Все элементы набора $\{(r_1 - r_2) \bmod \mathbb{Z} \mid r_1, r_2 \in S, r_1 \neq r_2\}$ являются различными.

СЛЕДСТВИЕ. U является Γ -модулем Фонтена–Лаффе с весами из промежутка $[0, p-2]$, удовлетворяющим условиям C1, C2 из § 1, если и только если $U \simeq \mathcal{U}(M)$, где $M \in \text{MF}^{(S)}$ и $S \subset R_p(p-2)$ удовлетворяет сформулированному выше свойству C4.

2.3. Функция n_M . Пусть $M \in \text{MF}^{(S)}$ задан в обозначениях из п. 2.2. Обозначим через v_p p -адический показатель кольца W такой, что $v_p(p) = 1$.

Определим функцию $n_M: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ следующим образом. Для $r, r' \in S$ положим

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

Тогда для $r_1, r_2 \in S$ соответствующее значение функции n_M задается с помощью равенства

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

ПРЕДЛОЖЕНИЕ. Функция n_M удовлетворяет следующим свойствам:

- 1) $n_M(r, r) \geq 1$ для любого $r \in S$;
- 2) $n_M(r_1(1), r_2(1)) = n_M(r_1, r_2)$ для любых $r_1, r_2 \in S$;
- 3) для любых $r_1, r_2, r_3 \in S$ выполнено неравенство

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

- 4) если $r_1, r_2 \in S$ и для всех $i \in \mathbb{Z}$ выполнено неравенство $l_0(r_1(i)) \geq l_0(r_2(i))$, то

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

ДОКАЗАТЕЛЬСТВО. Свойство 1) вытекает из свойства b_1) для коэффициентов $\beta_{rr'}$; 2) вытекает из равенств $n_M^*(r(1), r'(1)) = n_M^*(r, r')$; 3) вытекает из определения $n_M(r_1, r_2)$.

- 4) Если $n_M(r_1, r_2) = \infty$, то это равенство следует из свойства 3). Если $n_M(r_1, r_2) < \infty$, то

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

для некоторых $l \geq 1$ и $r^{(1)}, \dots, r^{(l)} \in S$, так как $n_M^*(r_1, r_2) = \infty$ согласно свойству b_2) из п. 2.2. Из определения функции n_M вытекает, что

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

Это дает

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

Теперь достаточно заметить, что согласно свойству 3) имеется неравенство

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

ЗАМЕЧАНИЕ. Из приведенного выше определения функции n_M не очень понятно, что оно зависит лишь от класса изоморфизма $M \in \text{MF}^{(S)}$ в категории MF . Это свойство может быть выведено из функториальности расщепления Винтенберже (см. [9]) или из теоремы А (см. п. 2.5 ниже).

2.4. Полулинейные функции и их графы.

2.4.1. Пусть S – конечное множество. Обозначим через Φ_S множество функций

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

таких, что для всех $r_1, r_2, r_3 \in S$ выполнены следующие свойства:

$$(1_\Phi) \quad n(r_1, r_1) \geq 1;$$

$$(2_\Phi) \quad n(r_1, r_2) \leq n(r_1, r_3) + n(r_3, r_2).$$

Если $S_1 \subset S \times S$ и $(r_1, r_2) \in S \times S$, то мы будем использовать обозначение $S_1(r_1, r_2)$ для множества последовательностей $(r_1, r^{(1)}, \dots, r^{(l)}, r_2)$ таких, что $l \geq 0$ и $(r_1, r^{(1)}), \dots, (r^{(l)}, r_2) \in S_1$ (в ориентированном графе с вершинами S и ребрами S_1 это множество является множеством всех путей, соединяющих r_1 и r_2).

Обозначим через $\mathcal{V}_S$ множество функций

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

где $S_v \subset S \times S$ и выполнены следующие два свойства:

$$(1_\mathcal{V}) \quad \text{если } l \geq 0, \quad r \in S \text{ и } (r, \dots, r^{(l)}, r) \in S_v(r, r), \text{ то}$$

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

$$(2_\mathcal{V}) \quad \text{если } (r_1, r_2) \in S_v \text{ и } (r_1, \dots, r^{(l)}, r_2) \in S_v(r_1, r_2), \text{ где } l \geq 1, \text{ то}$$

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

Таким образом, $\mathcal{V}_S$ является множеством ориентированных графов с данным множеством вершин S , снабженных неотрицательной целой метрикой, у которых ребра являются кратчайшими путями между их вершинами и не существует циклов длины 0.

Если $n \in \Phi_S$, пусть

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

и рассмотрим функцию $\pi(n): S^{(n)} \rightarrow \mathbb{Z}_{\geq 0}$ такую, что $\pi(n)(r_1, r_2) = n(r_1, r_2)$, где $(r_1, r_2) \in S^{(n)}$.

Проверим, что $\pi(n) \in \mathcal{V}_S$.

Действительно, свойства (1_Φ) и (2_Φ) для $n \in \Phi_S$ влекут свойство $(1_\mathcal{V})$ для функции $\pi(n)$. Если свойство $(2_\mathcal{V})$ не выполнено для $\pi(n)$, то существует путь $(r_1, r^{(1)}, \dots, r^{(l)}, r_2) \in S^{(n)}(r_1, r_2)$, где $l \geq 1$, такой, что

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

Отсюда следует, что $n(r_1, r_2) \geq n(r_1, r^{(1)}) + n(r^{(1)}, r_2)$, и мы получили $(r_1, r_2) \notin S^{(n)}$. Противоречие.

Итак, определено отображение $\pi: \Phi_S \rightarrow \mathcal{V}_S$.

Пусть $v \in \mathcal{V}_S$. Если $r_1, r_2 \in S$ и $S_v(r_1, r_2) = \emptyset$, то положим $\eta(v)(r_1, r_2) = \infty$. В противном случае положим

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

Очевидно, $\eta(v) \in \Phi_S$, и, таким образом, определено отображение $\eta: \mathcal{V}_S \rightarrow \Phi_S$.

2.4.2. Докажем следующее свойство.

ПРЕДЛОЖЕНИЕ. *Отображения π и η являются обратными друг к другу биекциями множеств Φ_S и $\mathcal{V}_S$.*

ДОКАЗАТЕЛЬСТВО. 1) Докажем сначала, что $\pi\eta = \text{id}_{\Phi_S}$. Пусть $n \in \Phi_S$ и $v = \pi(n) \in \mathcal{V}_S$. Покажем, что для любой пары $(r_1, r_2) \in S \times S$ выполнено равенство

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

Этот факт вытекает из следующей леммы.

ЛЕММА. а) Если $\eta(v)(r_1, r_2) < \infty$, то $n(r_1, r_2) \leq \eta(v)(r_1, r_2)$.

б) Если $n(r_1, r_2) < \infty$, то $\eta(v)(r_1, r_2) \leq n(r_1, r_2)$.

ДОКАЗАТЕЛЬСТВО. а) $\eta(v)(r_1, r_2) < \infty \Rightarrow S^{(n)}(r_1, r_2) \neq \emptyset \Rightarrow$

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

Из определения $v = \pi(n)$ вытекает, что $v(r_1, r^{(1)}) = n(r_1, r^{(1)}), \dots, v(r^{(l)}, r_2) = n(r^{(l)}, r_2)$ и, следовательно, $\eta(v)(r_1, r_2) \geq n(r_1, r_2)$.

б) Пусть $n(r_1, r_2) < \infty$. Тогда можно найти представление

$$n(r_1, r_2) = n(r_1, r^{(1)}) + \dots + n(r^{(l)}, r_2), \quad (1)$$

в котором $r^{(1)}, \dots, r^{(l)} \in S$, а число слагаемых $l + 1 = l(r_1, r_2)$ является максимально возможным.

Действительно, множество таких представлений без каких-либо условий на число их слагаемых непусто (можно взять $l = 0$). Но число этих слагаемых является заведомо ограниченным, так как для любых $r'_0, \dots, r'_{|S|} \in S$ выполнено неравенство

$$n(r'_0, r'_1) + \dots + n(r'_{|S|-1}, r'_{|S|}) \geq 1$$

(существуют $0 \leq i < j \leq |S|$ такие, что $r'_i = r'_j$, и тогда левая часть не меньше, чем $n(r'_i, r'_{i+1}) + \dots + n(r'_{j-1}, r'_j) \geq n(r'_i, r'_j) \geq 1$).

Из приведенного выше свойства максимальности представления (1) теперь вытекает, что $(r_1, r^{(1)}), \dots, (r^{(l)}, r_2) \in S^{(n)}$, следовательно, $S^{(n)}(r_1, r_2) \neq \emptyset$ и $\eta(v)(r_1, r_2) \leq n(r_1, r_2)$. Лемма доказана.

2) Докажем, что $\eta\pi = \text{id}_{\mathcal{V}_S}$. Пусть $v \in \mathcal{V}_S$ и $n = \eta(v) \in \Phi_S$. Непосредственно из определений множеств $\mathcal{V}_S$ и отображения η вытекает, что $n(r_1, r_2) = v(r_1, r_2)$ при $(r_1, r_2) \in S_v$. Таким образом,

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

Докажем, что $S_v \subset S^{(n)}$. Пусть $(r_1, r_2) \in S_v$ и $r_3 \in S$. Если либо $S_v(r_1, r_3) = \emptyset$, либо $S_v(r_3, r_2) = \emptyset$, то $n(r_1, r_2) < \infty = n(r_1, r_3) + n(r_3, r_2)$.

Если $S_v(r_1, r_3) \neq \emptyset$ и $S_v(r_3, r_2) \neq \emptyset$, то

$$\begin{aligned} n(r_1, r_3) &= v(r_1, r^{(1)}) + \dots + v(r^{(l_1)}, r_3), \\ n(r_3, r_2) &= v(r_3, r''^{(1)}) + \dots + v(r''^{(l_2)}, r_2) \end{aligned}$$

для некоторых путей $(r_1, r^{(1)}, \dots, r^{(l_1)}, r_3) \in S_v(r_1, r_3)$, $(r_3, r''^{(1)}, \dots, r''^{(l_2)}, r_2) \in S_v(r_3, r_2)$. Теперь из свойства $(2_{\mathcal{V}})$ получаем, что $n(r_1, r_2) < n(r_1, r_3) + n(r_3, r_2)$. Таким образом, $n(r_1, r_2) < n(r_1, r_3) + n(r_3, r_2)$ для всех $r_3 \in S$, т.е. $(r_1, r_2) \in S^{(n)}$.

Докажем, что $S^{(n)} \subset S_v$. Пусть $(r_1, r_2) \in S^{(n)}$; тогда $n(r_1, r_2) < \infty$, $S_v(r_1, r_2) \neq \emptyset$ и $n(r_1, r_2) = n(r_1, r^{(1)}) + \dots + n(r^{(l)}, r_2)$ для некоторого пути $(r_1, r^{(1)}, \dots, r^{(l)}, r_2) \in S_v(r_1, r_2)$. Если $l \geq 1$, то положим $r_3 = r^{(1)}$. Тогда $n(r^{(1)}, r^{(2)}) + \dots + n(r^{(l)}, r_2) \geq n(r_3, r_2)$ и $n(r_1, r_2) \geq n(r_1, r_3) + n(r_3, r_2)$. Значит, $(r_1, r_2) \notin S^{(n)}$. Противоречие. Следовательно, $l = 0$ и $(r_1, r_2) \in S_v$. Предложение доказано.

2.4.3. В §3 нам понадобится следующий критерий.

ПРЕДЛОЖЕНИЕ. Пусть $n_1, n_2 \in \Phi_S$ таковы, что:

- 1) $n_1(r_1, r_2) \geq n_2(r_1, r_2)$ для любых $r_1, r_2 \in S$;
 - 2) если $\pi(n_2) = v_2 \in \mathcal{V}_S$ и $(r_1, r_2) \in S_{v_2}$, то $n_1(r_1, r_2) \leq v_2(r_1, r_2)$.
- Тогда $n_1 = n_2$.

ДОКАЗАТЕЛЬСТВО. Пусть $v_1 = \pi(n_1) \in \mathcal{V}_S$. Тогда $S_{v_1} \supset S_{v_2}$.

Действительно, если $(r_1, r_2) \in S_{v_2}$, то

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

для всех $r_3 \in S$, т.е. $(r_1, r_2) \in S_{v_1}$.

Очевидно, $v_1|_{S_{v_2}} \leq v_2$. Для любого $(r_1, r_2) \in S \times S$ имеем

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

и, следовательно,

$$\begin{aligned} n_1(r_1, r_2) &= \eta(v_1)(r_1, r_2) \\ &= \min\{v_1(r_1, r^{(1)}) + \dots + v_1(r^{(l)}, r_2) \mid (r_1, \dots, r^{(l)}, r_2) \in S_{v_1}(r_1, r_2)\} \\ &\leq \min\{v_2(r_1, r^{(1)}) + \dots + v_2(r^{(l)}, r_2) \mid (r_1, \dots, r^{(l)}, r_2) \in S_{v_2}(r_1, r_2)\} \\ &= n_2(r_1, r_2). \end{aligned}$$

Предложение доказано.

2.4.4. Пусть S – конечное множество в R_p такое, что $r \in S$ влечет $r(1) \in S$. Пусть $n \in \Phi_S$ и $\pi(n) = v \in \mathcal{V}_S$. Из приведенного выше описания соответствия $n \leftrightarrow v$ вытекает следующее предложение.

ПРЕДЛОЖЕНИЕ. Следующие утверждения являются эквивалентными:

1) а) для произвольных $r_1, r_2 \in S$ выполнено равенство

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

б) если $r_1, r_2 \in S$ и $l_0(r_1(i)) \geq l_0(r_2(i))$ для всех $i \in \mathbb{Z}$, то

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

2) а) если $(r_1, r_2) \in S_v$, то существует $i \in \mathbb{Z}$ такое, что $l_0(r_1(i)) < l_0(r_2(i))$ (в частности, $(r, r) \notin S_v$ для любого $r \in S$);

б) если $(r_1, r_2) \in S_v$, то $(r_1(1), r_2(1)) \in S_v$ и

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

ЗАМЕЧАНИЕ. Используем отождествление множества характеров группы Γ_{tr} с множеством R_p , заданное с помощью соответствия $\chi \mapsto r(\chi)$ из п. 2.1. Тогда множество функций $\mathcal{F}_S$ отождествляется с подмножеством в Φ_S , состоящим из функций n таких, что для любых $r_1, r_2 \in S$ выполнены свойства

$$\begin{aligned} n(r_1, r_2) &= n(r_1(1), r_2(1)), \\ n(r_1, r_1) &= \min\{n(r_1, r) + n(r, r_2) \mid r \in S\}. \end{aligned}$$

При этом подмножество $\eta(\mathcal{F}_S) \subset \mathcal{V}_S$ характеризуется условием $(r, r) \notin S_v$ для любого $r \in S$ и условием 2), б) из сформулированного выше предложения.

2.5. Основные утверждения. Пусть $S \subset R_p(p-2)$ – конечное множество такое, что $r \in S \Rightarrow r(1) \in S$, и S удовлетворяет условию С4 из п. 2.2.

2.5.1. Пусть $M \in \text{MF}^{(S)}$ и $U = \mathcal{U}(M)$. Если $H(M)$ – образ группы Γ в $\text{Aut}_{\mathbb{Z}_p} U$, то $S = S_U$ (см. п. 2.2), и согласно предложению п. 1.2 имеется функция

$$n_U: S \times S \longrightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

Пусть $n_M: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ – функция, определенная в п. 2.3.

ТЕОРЕМА А. Во введенных выше обозначениях имеет место равенство $n_U = n_M$.

Мы докажем эту теорему ниже, в § 3.

2.5.2. Пусть функция $n: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ такова, что для произвольных $r_1, r_2, r_3 \in S$ выполнены следующие свойства:

- а) $n(r_1, r_1) \geq 1$;
- б) $n(r_1, r_2) = n(r_1(1), r_2(1))$;
- в) $n(r_1, r_2) \leq n(r_1, r_3) + n(r_3, r_2)$;
- г) $n(r_1, r_1) = \min\{n(r_1, r) + n(r, r_1) \mid r \in S\}$.

Построим $\mathbb{Z}_p[\Gamma_{\text{tr}}]$ -модуль U такой, что $\text{rk}_{\mathbb{Z}_p} U = |S|$ и $S_U = S$. Очевидно, функция n принадлежит множеству $\mathcal{F}_{S_U}$. Пусть гомоморфизм $\rho_1: \Gamma_{\text{tr}} \rightarrow \text{Aut}_{\mathbb{Z}_p} U$ задает структуру Γ_{tr} -модуля на U . Тогда $\rho_1(\Gamma_{\text{tr}}) = H_1$ — циклическая группа порядка, взаимно простого с p . Пусть группа $G \in \text{Gr}_U$ такова, что для соответствующей функции $n_G \in \mathcal{F}_{S_U}$ имеем $n_G = n$. Можно проверить, что гомоморфизм ρ_1 может быть продолжен до гомоморфизма $\rho: \Gamma \rightarrow \text{Aut}_{\mathbb{Z}_p} U$ (т.е. $\rho_1 = s \circ \rho$, где $s: \Gamma_{\text{tr}} \rightarrow \Gamma$ — фиксированное сечение естественной проекции Γ на Γ_{tr}) такого, что образ $\rho(\Gamma)$ совпадает с полупрямым произведением групп H_1 и G . Это означает, что любая функция $n \in \mathcal{F}_S$ возникает из некоторого $\mathbb{Z}_p[\Gamma]$ -модуля U .

Если $U = \mathcal{U}(M)$, где $M \in \text{MF}^{(S)}$, то предложение п. 2.3 и сформулированная выше теорема А показывают, что функция $n = n_U$ удовлетворяет следующему свойству d'), которое является более строгим по сравнению со свойством d):

d') если $r_1, r_2 \in S$ и $l_0(r_1(i)) \geq l_0(r_2(i))$ для всех $i \in \mathbb{Z}$, то

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

ТЕОРЕМА В. Если функция $n: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ удовлетворяет свойствам а)–с) и d') (см. выше), то существует $M \in \text{MF}^{(S)}$ такой, что $n = n_{\mathcal{U}(M)}$.

ДОКАЗАТЕЛЬСТВО. Пусть $\pi(n) = v \in \mathcal{V}_S$. Согласно свойству 2), б) из предложения п. 2.4.4 множество S_v инвариантно относительно сдвига $(r_1, r_2) \mapsto (r_1(1), r_2(1))$. Рассмотрим разложение множества S_v в объединение непересекающихся орбит относительно этого сдвига. Фиксируем в каждой орбите некоторую пару (r_1, r_2) такую, что $l_0(r_1) < l_0(r_2)$ (это возможно благодаря свойству 2), а) предложения п. 2.4.4), и выберем $\beta_{r_2 r_1}^0 \in W$ такой, что $v_p(\beta_{r_2 r_1}^0) = v(r_1, r_2)$. Для всех остальных элементов (r_1, r_2) из множества $S \times S$ положим $\beta_{r_2 r_1}^0 = 0$.

Покажем, что существует $M \in \text{MF}^{(S)}$, заданный в обозначениях из п. 2.2 с помощью выбранных таким образом коэффициентов $\beta_{r_2 r_1}^0$, $r_1, r_2 \in S$.

Если $r, r' \in S$ и $l_0(r) \geq l_0(r')$, то, очевидно, $\beta_{r' r}^0 = 0$, и условие b2) из п. 2.2 выполнено.

Чтобы вывести условие b1) из п. 2.2, положим для любых $r, r' \in S$ $r \succ r'$, если $n(r, r') = 0$, и $r \not\succ r'$ в противном случае, т.е. если $n(r, r') > 0$.

Свойства функции n влекут следующие свойства отношения $\succ$:

- 1) $r \not\succ r$ для любого $r \in S$;
- 2) $r_1 \succ r_2, r_2 \succ r_3 \Rightarrow r_1 \succ r_3$ для любых $r_1, r_2, r_3 \in S$;
- 3) $r_1 \succ r_2 \Leftrightarrow r_1(1) \succ r_2(1)$ для любых $r_1, r_2 \in S$.

Пусть $S = \{r_1, \dots, r_1(h_1 - 1); \dots; r_m, \dots, r_m(h_m - 1)\}$ (см. обозначения п. 2.2, b1)).

Из свойств 1) и 2) следует существование строго минимального (относительно отношения порядка $\succ$) элемента $r_{j_m}(\alpha_0)$, где $1 \leq j_m \leq m$ и $\alpha_0 \in \mathbb{Z}/h_{j_m}\mathbb{Z}$. Иными словами, $r_{j_m}(\alpha_0) \not\succ r$ для произвольного $r \in S$. Согласно свойству 3) мы имеем также, что $r_{j_m}(\alpha) \not\succ r$ для всех $\alpha \in \mathbb{Z}/h_{j_m}\mathbb{Z}$ и $r \in S$.

Применим аналогичную процедуру к множеству

$$S_{j_m} = S \setminus \{r_{j_m}(\alpha) \mid \alpha \in \mathbb{Z}/h_{j_m}\mathbb{Z}\}.$$

Мы получим индекс $1 \leq j_{m-1} \leq m$ такой, что $j_{m-1} \neq j_m$, и для всех $\alpha \in \mathbb{Z}/h_{j_{m-1}}\mathbb{Z}$ и $r \in S_{j_m}$ выполнено $r_{j_{m-1}}(\alpha) \neq r$. Повторяя этот процесс, мы получим подстановку $\begin{pmatrix} 1 & \dots & m \\ j_1 & \dots & j_m \end{pmatrix}$ такую, что если $r = r_{j_a}(\alpha)$, $r' = r_{j_b}(\beta)$, $a \geq b$, $\alpha \in \mathbb{Z}/h_{j_a}\mathbb{Z}$ и $\beta \in \mathbb{Z}/h_{j_b}\mathbb{Z}$, то $r \neq r'$, т.е. $n(r, r') > 0$.

Если во введенных выше обозначениях $\beta_{r',r}^0 \neq 0$, то $(r, r') \in S_v$ и $v_p(\beta_{r',r}^0) = v(r, r') = n(r, r') > 0$, т.е. $\beta_{r',r}^0 \in pW$, и условие b_1) выполнено. Если $\beta_{r',r}^0 = 0$, то условие b_1) выполнено по тривиальным соображениям.

Осталось заметить, что по построению функция $\pi(n): S_v \rightarrow \mathbb{Z}_{\geq 0}$ совпадает с ограничением на S_v функции n_M^* из п. 2.3. Так как для любого $(r_1, r_2) \in S \times S \setminus S_v$ мы имеем $n^*(r_1, r_2) = \infty$, то из определения функции n_M следует, что $n_M = \eta(n_M^*)$ для отображения $\eta: \mathcal{V}_S \rightarrow \Phi_S$ из п. 2.4.1. Окончательно из предложения п. 2.4.2 получаем, что

$$n_M = \eta(n_M^*) = \eta(\pi(n)) = n.$$

Теорема В доказана.

2.5.3. Рассмотрим случай, когда $U = \mathcal{U}(M)$, где $M \in \text{MF}^{(S)}$, является простым $s(\Gamma_{\text{tr}})$ -модулем. Это означает, что

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

где $r \in R_p(p-2)$ и $h = h(r)$, т.е. последовательность $\{l_s(r)\}_{s \geq 1}$ p -ичных цифр для r имеет минимальный положительный период h . Пусть χ — характер группы Γ_{tr} такой, что $r(\chi) = r$. Согласно предложению п. 1.1 мы имеем следующую импликацию:

$$\text{ord } \chi = p^h - 1 \Rightarrow S \text{ удовлетворяет условию C4.}$$

Покажем, что при этих предположениях условие d') совпадает с условием d).

Действительно, пусть $r_1, r_2 \in S$ таковы, что $l_0(r_1(i)) \geq l_0(r_2(i))$ для всех $i \in \mathbb{Z}$. Выберем $\alpha \in \mathbb{Z}$ такое, что $r_2 = r_1(\alpha)$. Тогда для любого $i \in \mathbb{Z}$ условие d') влечет

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

Следовательно, $l_0(r_1(i)) = l_0(r_1(i + \alpha))$ для всех $i \in \mathbb{Z}$. Это дает $\alpha \equiv 0 \pmod{h}$ и $r_2 = r_1$. Таким образом, используя данное в п. 1.4 описание функций, принадлежащих множеству $\mathcal{F}_S$, мы получаем следующее предложение.

ПРЕДЛОЖЕНИЕ. Пусть $r \in R_p(p-2)$ таково, что $r = l/(p^h - 1)$, где $l \in \mathbb{N}$ и $\text{н.о.д.}(l, p^h - 1) = 1$. Пусть $S = \{r, r(1), \dots, r(h-1)\}$, и предположим, что функция $n: \mathbb{Z}/h\mathbb{Z} \rightarrow \mathbb{N} \cup \{\infty\}$ такова, что

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

$$n(i + j) \leq n(i) + n(j) \quad \text{для всех} \quad i, j \in \mathbb{Z}/h\mathbb{Z}.$$

Тогда существует $M \in \text{MF}^{(S)}$ такой, что $n_{\mathcal{U}(M), \chi} = n$ (где χ — характер группы Γ_{tr} такой, что $r(\chi) = r$).

2.5.4. В обозначениях из п. 2.5.3 допустим, что $r \in R_p(p-2)$ удовлетворяет предположению С5 из п. 3.12 (см. ниже), т.е. многочлены $l_1(r)X^{p^{h-1}} + \dots + l_h(r)X$ и $X^{p^{h-1}} - 1$ являются взаимно простыми в кольце $\mathbb{F}_p[X]$. Согласно следствию из п. 3.12 (см. ниже) в этом случае функция n_U полностью определяет образ группы Галуа в $\text{Aut}_{\mathbb{Z}_p} U$.

Сформулированные выше предположения естественно реализуются в следующей ситуации.

Пусть $p > 2$ и $\mathcal{G}$ – формальная группа над W , имеющая конечную высоту h . Тогда ее модуль Тейта $U = T(\mathcal{G})$ является Γ -модулем Фонтена–Лаффе с весами 0 и 1. Пусть $\mathcal{G}$ – 1-мерная формальная группа. Тогда слабо разветвленный характер χ_h^* (см. п. 2.2) принадлежит множеству $S_U = \{p^i/(p^h - 1) \mid 0 \leq i < h\}$. Следовательно, предложение из п. 2.5.3 дает положительный ответ на вопрос Ж.-М. Фонтена из работы [5] о реализации произвольного элемента множества $\mathcal{F}_{S_U}$ с помощью некоторой 1-мерной формальной группы $\mathcal{G}$ над кольцом W (частные случаи этой проблемы рассматривались в работах [8], [4], [3]). Очевидно, дополнительное предположение С5 здесь тоже выполнено, и мы получаем следующее утверждение.

ПРЕДЛОЖЕНИЕ. Пусть $h \in \mathbb{N}$ и H – замкнутая подгруппа в $\text{Aut}_{\mathbb{Z}_p} W(\mathbb{F}_{p^h})$. Тогда следующие утверждения являются эквивалентными:

- 1) существуют 1-мерная формальная группа $\mathcal{G}$ высоты h , определенная над W , и изоморфизм $\mathbb{Z}_p$ -модулей $T(\mathcal{G}) \simeq W(\mathbb{F}_{p^h})$, который преобразует образ $H(\mathcal{G})$ группы Γ в $\text{Aut}_{\mathbb{Z}_p} T(\mathcal{G})$ на H ;
- 2) H является расширением циклической группы порядка, взаимно простого с p , с помощью про- p -группы и $H \supset W(\mathbb{F}_{p^h})^* \text{id}_{W(\mathbb{F}_{p^h})}$.

ЗАМЕЧАНИЕ. Можно использовать связь между фильтрованными модулями, связанными с рассмотренными выше формальными группами $\mathcal{G}$ и функциональными уравнениями для их логарифмов (см. [6, гл. 5]), для получения явного выражения для соответствующей функции $n_{T(\mathcal{G}), \chi_h^*}$ в следующем виде. Пусть $l_{\mathcal{G}}(X) \in W_{\mathbb{Q}_p}[[X]]$ – логарифм формальной группы $\mathcal{G}$, который удовлетворяет функциональному уравнению

$$l_{\mathcal{G}}(X) = X + \frac{1}{p} \left(\alpha_1 \sigma_* l_{\mathcal{G}}(X^p) + \dots + \alpha_h \sigma_*^h l_{\mathcal{G}}(X^{p^h}) \right),$$

где σ_* обозначает действие абсолютного морфизма Фробениуса на коэффициенты степенного ряда, $\alpha_1, \dots, \alpha_{h-1} \in pW$ и $\alpha_h \in W^*$. Тогда для любого $i \in \mathbb{Z}/h\mathbb{Z}$ мы имеем

$$n_{T(\mathcal{G}), \chi_h^*}(i) = \min \{ v_p(\alpha_{i_1}) + \dots + v_p(\alpha_{i_s}) \mid s \in \mathbb{N}, 1 \leq i_1, \dots, i_s < h, (i_1 + \dots + i_s) \bmod h = i \}.$$

§ 3. Доказательство теоремы А

3.1. Пусть фильтрованный модуль $M \in \text{MF}^{(S)}$ задан в обозначениях п. 2.2. Выберем $r_1, \dots, r_m \in S$ такие, что

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

где $h_j = h(r_j)$ являются (как и ранее) минимальными положительными периодами p -ичных разложений чисел r_j , $1 \leq j \leq m$.

Выберем $N \in \mathbb{N}$ такое, что $N \equiv 0 \pmod{h_j}$ для всех $1 \leq j \leq m$.

Для любых $1 \leq j, j' \leq m$ и $i, i' \in \mathbb{Z}/N\mathbb{Z}$ выберем $\beta_{(r_j, i), (r_{j'}, i')} \in W$ таким образом, чтобы для всех $r \in S$ выполнялись равенства

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

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

(как и ранее, v_p — p -адический показатель кольца W такой, что $v_p(p) = 1$).

Определим фильтрованный модуль $M^* \in \text{MF}_f$ следующим образом:

- 1) M^* имеет W -базис $\{m_{(r_j, i)} \mid 1 \leq j \leq m, i \in \mathbb{Z}/N\mathbb{Z}\}$;
- 2) для $0 \leq l < p$ подмодуль M^{*l} фильтрации в M^* порожден элементами множества

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

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

- 3) для $0 \leq l < p$ σ -линейные морфизмы $\phi_l: M^{*l} \rightarrow M^*$ определены однозначно с помощью соотношений

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

Можно легко проверить, что соответствие

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

задает инъективный морфизм $i_{M, M^*}: M \rightarrow M^*$ в категории MF_f .

3.2. Из определения функтора $\mathcal{U}$ вытекает, что соответствие

$$u \mapsto (m_r(u))_{r \in S} \in \bigoplus_{r \in S} A_{\text{cris}}$$

задает инъективный морфизм Γ -модулей

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

Более того, W -линейное продолжение морфизма κ

$$\kappa_W: \mathcal{U}(M) \otimes W \longrightarrow \bigoplus_{r \in S} A_{\text{cris}}$$

является по-прежнему инъективным.

Относительно вложения κ модуль $\mathcal{U}(M)$ отождествляется с $\mathbb{Z}_p[\Gamma]$ -модулем наборов $(u_r)_{r \in S} \in \bigoplus_{r \in S} A_{\text{cris}}$ таких, что для любого $r \in S$ выполнено

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

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

Аналогично, модуль Галуа $\mathcal{U}(M^*)$ может быть отождествлен с множеством наборов $(u_{(r_j, i)})_{1 \leq j \leq m, i \in \mathbb{Z}/N\mathbb{Z}}$ таких, что для любых $1 \leq j \leq m$ и $i \in \mathbb{Z}/N\mathbb{Z}$ выполнено

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

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

Эпиморфизм $\mathcal{U}(i_{M, M^*}): \mathcal{U}(M^*) \rightarrow \mathcal{U}(M)$ и его W -линейное продолжение индуцированы гомоморфизмом

$$\bigoplus_{\substack{1 \leq j \leq m \\ i \in \mathbb{Z}/N\mathbb{Z}}} A_{\text{cris}} \longrightarrow \bigoplus_{r \in S} A_{\text{cris}}$$

таким, что $(a_{(r_j, i)})_{1 \leq j \leq m, i \in \mathbb{Z}/N\mathbb{Z}} \mapsto (a_r)_{r \in S}$, где $a_r = \sum_{r_j(i)=r} a_{(r_j, i)}$.

Если $\mathcal{U}(M) \otimes W = \bigoplus_{\chi} U(M)_{\chi}$ и $\mathcal{U}(M^*) \otimes W = \bigoplus_{\chi} \mathcal{U}(M^*)_{\chi}$ – разложения $s(\Gamma_{\text{tr}})$ -модулей по характерам χ группы $s(\Gamma_{\text{tr}})$, то для любого χ имеется индуцированное эпиморфное отображение W -модулей

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

3.3. Для $1 \leq j_0, \dots, j_s, \dots \leq m$ и $a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ определим объекты $M^*(j_0), M^*(j_1, b_1; a_0, j_0), \dots, M^*(j_s, b_s; a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0)$ категории MF_f следующим образом.

$M^*(j_0)$ имеет W -базис $\{m(i, j_0) \mid i \in \mathbb{Z}/N\mathbb{Z}\}$, для $0 \leq l < p$ его подмодуль фильтрации $M^*(j_0)^l$ порожден элементами множеств $\{m(i, j_0) \mid l_i(r_{j_0}) \geq l\}$, σ -линейные морфизмы $\phi_l: M^*(j_0)^l \rightarrow M^*(j_0)$ однозначно определены с помощью соотношений

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

Если $s \geq 1$, то $M^*(j_s, b_s; \dots; a_0, j_0)$ имеет W -базис

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

для $0 \leq l' < p$ его подмодуль фильтрации $M^*(j_s, b_s; \dots; a_0, j_0)^{l'}$ порожден элементами множества

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

σ -линейные морфизмы $\phi_{l'}: M^*(j_s, b_s; \dots; a_0, j_0)^{l'} \rightarrow M^*(j_s, b_s; \dots; a_0, j_0)$ однозначно определены условиями

$$\begin{aligned} \phi_{l_{i-1}(r_{j_l})}(m(i-1, j_l, b_l; \dots; a_0, j_0)) &= m(i, j_l, b_l; \dots; a_0, j_0) \\ &+ \delta(i, b_l) \beta_{(r_{j_l}, b_l), (r_{j_{l-1}}, a_{l-1})}^* m(a_{l-1}, j_{l-1}, b_{l-1}; \dots; a_0, j_0), \end{aligned}$$

где $l \geq 1$, δ – символ Кронекера, и

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

(напомним, что для любых $r, r' \in S$ мы имеем $n_M^*(r, r') = \min\{v_p(\beta_{r'(i)r(i)}) \mid i \in \mathbb{Z}\}$, и если $n_M^*(r_{j_{l-1}}(a_{l-1}), r_{j_l}(b_l)) = \infty$, то $\beta_{(r_{j_l}, b_l), (r_{j_{l-1}}, a_{l-1})}^* = 0$).

Для любого $s \geq 1$ имеются естественные инъективные морфизмы в категории MF_f

$$M^*(j_{s-1}, b_{s-1}; \dots; a_0, j_0) \longrightarrow M^*(j_s, b_s; \dots; a_0, j_0). \quad (2)$$

Если $U^*(j_s, b_s; \dots; a_0, j_0) = \mathcal{U}(M^*(j_s, b_s; \dots; a_0, j_0))$, то имеется m проективных систем $\mathbb{Z}_p[\Gamma]$ -модулей

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

где все связывающие морфизмы

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

являются сюръективными морфизмами $\mathbb{Z}_p[\Gamma]$ -модулей, которые получаются применением функтора Фонтена–Лаффе к инъективным морфизмам (2).

3.4. Пусть $1 \leq j_0 \leq m$; тогда согласно аргументам из п. 3.2 соответствие

$$\kappa_{j_0}: u^* \mapsto (m(i, j_0)(u^*))_{i \in \mathbb{Z}/N\mathbb{Z}} \in \bigoplus_{i \in \mathbb{Z}/N\mathbb{Z}} A_{\text{cris}}$$

задает отождествление $U^*(j_0)$ с $\mathbb{Z}_p[\Gamma]$ -подмодулем в $\bigoplus_{i \in \mathbb{Z}/N\mathbb{Z}} A_{\text{cris}}$, состоящим из $(u_i)_{i \in \mathbb{Z}/N\mathbb{Z}}$ таких, что $u_i \in A_{\text{cris}}^{l_i(r_{j_0})}$ и $\phi_{l_{i-1}(r_{j_0})}(u_{i-1}) = u_i$ для всех $i \in \mathbb{Z}/N\mathbb{Z}$.

Фиксируем некоторый $u^*(j_0) \in U^*(j_0) \setminus pU^*(j_0)$. Если

$$\kappa_{j_0}(u^*(j_0)) = (u^*(i, j_0))_{i \in \mathbb{Z}/N\mathbb{Z}},$$

то

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

где $q = p^N$.

Если $\tau \in s(\Gamma_{\text{tr}})$, то $\tau u^*(i, j_0) = \chi_i^{(j_0)}(\tau) u^*(i, j_0)$, где $\chi_i^{(j_0)}$ – характер группы $s(\Gamma_{\text{tr}})$ с инвариантом $r(\chi_i^{(j_0)}) = r_{j_0}(i)$.

Действительно, этот факт может быть проверен с помощью вычисления характера $\tau \mapsto \chi_i^{(j_0)}(\tau) \bmod p$. Но $U^*(j_0) \otimes \mathbb{F}_p = \mathcal{U}(M^*(j_0) \otimes k)$ может быть описан с помощью явной конструкции значений функтора Фонтена–Лаффе на уровне объектов, аннулируемых умножением на p (см. п. 2.1).

В действительности $\tau u^*(i, j_0) = \eta_i^{(j_0)}(\tau) u^*(i, j_0)$ для любого $\tau \in \Gamma$, где $\eta_i^{(j_0)}: \Gamma \rightarrow W(\mathbb{F}_q)^*$ – непрерывный гомоморфизм такой, что $\eta_i^{(j_0)}|_{s(\Gamma_{\text{tr}})} = \chi_i^{(j_0)}$. Этот гомоморфизм может быть вычислен следующим образом.

Пусть G_N^{LT} – группа Любина–Тейта над $W(\mathbb{F}_q)$ с логарифмом

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

Действие группы Галуа Γ на модуле Тейта $T(G_N^{LT})$ задается с помощью непрерывного гомоморфизма

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

Если I_0^{ab} – подгруппа инерции группы Галуа максимального абелевого расширения поля частных кольца $W(\mathbb{F}_q)$, то имеется естественная проекция $\Gamma \rightarrow I_0^{\text{ab}}$ и отождествление теории полей классов $I_0^{\text{ab}} = W(\mathbb{F}_q)^*$. В этих терминах гомоморфизм η_{LT} равен композиции

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

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

Используем временно следующие более простые обозначения: $r = r_{j_0}$, $M^*(j_0) = M^*$, $u^*(j_0) = u^*$, $u^*(i, j_0) = u^*(i)$ и $\eta_i^{(j_0)} = \eta_i$. Таким образом, для любых $i \in \mathbb{Z}/N\mathbb{Z}$ и $\tau \in \Gamma$ мы имеем $\tau u^*(i) = \eta_i(\tau) u^*(i)$ и $\eta_i(\tau) = \sigma^i \eta_0(\tau)$.

ЛЕММА. $\eta_0 = \prod_{0 \leq i < N} (\sigma^{-i} \eta_{LT})^{l_i(r)}$.

ДОКАЗАТЕЛЬСТВО. Модуль Тейта $T = T(G_N^{LT})$ является $\mathbb{Z}_p[\Gamma]$ -модулем Фонтена–Лаффе, и мы можем использовать следующую явную конструкцию фильтрованного W -модуля $M_0 \in \text{MF}_f$ такого, что $\mathcal{U}(M_0) = T$ (см. [1]).

Пусть $o = (o_n)_{n \geq 0} \in T$, где $o_n \in G_N^{LT}(\overline{m})$ ($\overline{m}$ – максимальный идеал кольца нормирования $\overline{O}$ поля $\overline{K}$), $[p]o_{n+1} = o_n$ для $n \geq 0$ и $o_0 = 0$ (здесь $[p] = p \text{id}_{G_N^{LT}} \in \text{End } G_N^{LT}$). Если $\hat{o}_n \in A_{\text{cris}}$ – подъем $o_n \bmod p \in \overline{m} \bmod p\overline{O}$ по отношению к редукции по модулю p $A_{\text{cris}} \rightarrow \overline{O}/p\overline{O}$ структурного морфизма из определения A_{cris} , то можно показать, что соответствие

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

дает корректно определенный морфизм $m_0^{(0)} \in \text{Hom}_{\mathbb{Z}_p[\Gamma] \text{-mod}}(T, A_{\text{cris}}^1)$, причем $\sigma^N m_0^{(0)} = p m_0^{(0)}$ и

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

где $m_i^{(0)} = \sigma^{\hat{i}} m_0^{(0)} / p$ для $0 < \hat{i} \leq N$ такого, что $\hat{i} \bmod N = i$.

Из этой конструкции вытекает, что для произвольных $o \in T$ и $\tau \in \Gamma$ имеется равенство

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

Пусть $o = (o_n)_{n \geq 0} \in T$ таков, что $o_1 \neq 0$. Тогда $v = m_0^{(0)}(o) \in A_{\text{cris}}^1$, $\tau v = \eta_{LT}(\tau) v$ для всех $\tau \in \Gamma$ и $\sigma^N v = p v$.

Теперь легко проверяется, что для всех $i \in \mathbb{Z}/N\mathbb{Z}$

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

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

Это дает $u' = (u'(i))_{i \in \mathbb{Z}/N\mathbb{Z}} \in \kappa(\mathcal{U}(M^*))$, $u'(0) = w u^*(0)$ для некоторого $w \in W(\mathbb{F}_q)^*$ и $\tau u'(0) = \eta_0(\tau) u'(0)$ для $\tau \in \Gamma$. С другой стороны,

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

Лемма доказана.

3.5. Мы имеем следующее предложение.

ПРЕДЛОЖЕНИЕ. Для $1 \leq j_0, \dots, j_s, \dots \leq m$ и $i, a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ существуют элементы $u(i, j_0), \dots, u(i, j_s, b_s; \dots; a_0, j_0), \dots \in A_{\text{cris}}$ такие, что:

1) $u(i, j_0) \in A_{\text{cris}}^{l_i(r_{j_0})}$ и для $s \geq 1$

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

2) $\phi_{l_{i-1}(r_{j_0})}(u(i-1, j_0)) = u(i, j_0)$ и для $s \geq 1$

$$\begin{aligned} \phi_{l_{i-1}(r_{j_s})}(u(i-1, j_s, b_s; \dots; a_0, j_0)) &= u(i, j_s, b_s; \dots; a_0, j_0) \\ &+ \delta(i, b_s) \beta_{(r_{j_s}, b_s), (r_{j_{s-1}}, a_{s-1})} u(a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0); \end{aligned}$$

3) для любого $\tau \in s(\Gamma_{\text{tr}})$

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

где $\chi_{i, b_s, \dots, a_0}^{(j_0)}$ – характер группы $s(\Gamma_{\text{tr}})$ с инвариантом

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

4) $v_p(u(i, j_0)) = 0$ и для $s \geq 1$

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

ДОКАЗАТЕЛЬСТВО. Пусть $1 \leq j_0 \leq m$. Рассмотрим проективную систему $\mathcal{L}_{j_0}$ из п. 3.3. Мы хотим построить согласованную систему элементов

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

такую, что $u^*(j_0) \in U^*(j_0) \setminus pU^*(j_0)$ (см. п. 3.4), и если

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

то для любого $\tau \in s(\Gamma_{\text{tr}})$ имеется равенство

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

В действительности случай $s = 0$ был уже рассмотрен в п. 3.4.

По индукции можно предположить, что эти точки уже построены для всех $l < s$.

Возьмем $\hat{u}(j_s, b_s; \dots; a_0, j_0) \in U^*(j_s, b_s; \dots; a_0, j_0)$ так, чтобы

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

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

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

Тогда

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

$$\begin{aligned} \phi_{l_{i-1}(r_{j_s})}(\hat{u}(i-1, j_s, b_s; \dots; a_0, j_0)) &= \hat{u}(i, j_s, b_s; \dots; a_0, j_0) \\ &+ \delta(i, b_s) \beta_{(r_{j_s}, b_s), (r_{j_{s-1}}, a_{s-1})}^* u^*(a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0). \end{aligned} \quad (3)$$

Возьмем разложение по χ -компонентам

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

где χ пробегает множество характеров группы $s(\Gamma_{\text{tr}})$. Очевидно, ненулевые компоненты могут появиться только для характеров χ таких, что $r(\chi) \in S$ (в частности, эти характеры должны удовлетворять равенству $\sigma^N \chi = \chi$).

Положим

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

Тогда сравнение χ -компонент равенства (3) дает

$$\begin{aligned} \phi_{i_{i-1}(r_{j_s})}(u^*(i-1, j_s, b_s; \dots; a_0, j_0)) &= u^*(i, j_s, b_s; \dots; a_0, j_0) \\ &+ \delta(i, b_s) \beta_{(r_{j_s}, b_s), (r_{j_{s-1}}, a_{s-1})}^* u^*(a_{s-1}, j_{s-1}, b_{s-1}; \dots; a_0, j_0). \end{aligned}$$

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

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

Легко видеть, что $u^*(j_s, b_s; \dots; a_0, j_0) \mapsto u^*(j_{s-1}, b_{s-1}; \dots; a_0, j_0)$, и согласно нашей конструкции эти точки удовлетворяют свойствам из начала доказательства.

Теперь соотношение

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

задает семейство элементов кольца A_{cris} , которые удовлетворяют свойствам нашего предложения.

3.6. Для $1 \leq j_0 \leq m$ рассмотрим набор

$$u^{(j_0)} = (u_{(r_j, i)}^{(j_0)}) \in \bigoplus_{\substack{1 \leq j \leq m \\ i \in \mathbb{Z}/N\mathbb{Z}}} (A_{\text{cris}})_{(r_j, i)},$$

где

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

а сумма берется по всем $s \geq 0$, $1 \leq j_1, \dots, j_{s-1} \leq m$ и $b_s, a_{s-1}, \dots, b_1, a_0 \in \mathbb{Z}/N\mathbb{Z}$.

Легко проверяется, что для любого $1 \leq j_0 \leq m$

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

Более общо, если $w \in W(\mathbb{F}_q)$ и $q = p^N$, то пусть

$$w * u_{(r_j, i)}^{(j_0)} = (w * u_{(r_j, i)}^{(j_0)})_{1 \leq j \leq m, i \in \mathbb{Z}/N\mathbb{Z}},$$

где

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

а сумма берется по всем $s \geq 0$, $1 \leq j_1, \dots, j_{s-1} \leq m$, $b_s, a_{s-1}, \dots, b_1, a_0 \in \mathbb{Z}/N\mathbb{Z}$ и $\alpha(i, b_s, \dots, a_0) = i - b_s + a_{s-1} - \dots - b_1 + a_0$.

Тогда

$$\kappa(\mathcal{U}(M^*)) = \left\{ \sum_{1 \leq j_0 \leq m} w_{j_0} * u_{(r_j, i)}^{(j_0)} \mid w_1, \dots, w_m \in W(\mathbb{F}_q) \right\}.$$

Для $1 \leq j_0, j \leq m$ и $i_0, i \in \mathbb{Z}/N\mathbb{Z}$ положим

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

где сумма берется по всем наборам $(i, j_s, b_s; \dots; a_0, j_0)$ таким, что $j_s = j$ и $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

Тогда

$$u_{(r_j, i)}^{(j_0)} = \sum_{i_0 \in \mathbb{Z}/N\mathbb{Z}} u_{(j, i)}^{(j_0, i_0)},$$

для произвольного $w \in W(\mathbb{F}_q)$ выполнено

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

а для любого $\tau \in s(\Gamma_{\text{tr}})$ имеем

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

где $\chi_{i_0}^{(j_0)}$ – характер группы $s(\Gamma_{\text{tr}})$ с инвариантом $r(\chi_{i_0}^{(j_0)}) = r_{j_0}(i_0)$.

В использованных выше обозначениях $\kappa(\mathcal{U}(M^*))$ является Γ -модулем наборов

$$(u_{(j, i)}^*) \in \bigoplus_{\substack{1 \leq j \leq m \\ i \in \mathbb{Z}/N\mathbb{Z}}} (A_{\text{cris}})_{(r_j, i)}$$

таких, что

$$u_{(j, i)}^* = \sum_{\substack{i_0 \in \mathbb{Z}/N\mathbb{Z} \\ 1 \leq j_0 \leq m}} \sigma^{i_0}(w_{j_0}) u_{(j, i)}^{(j_0, i_0)},$$

где $w_1, \dots, w_m$ пробегают элементы $W(\mathbb{F}_q)$.

Пусть χ – характер группы $s(\Gamma_{\text{tr}})$ такой, что $r(\chi) \in S$. Тогда существуют единственные $1 \leq j_\chi \leq m$ и $i_\chi \in \mathbb{Z}/h_{j_\chi}\mathbb{Z}$ такие, что $r(\chi) = r_{j_\chi}(i_\chi)$. В этих терминах морфизм $\kappa_W = \kappa \otimes W$ отождествляет W -модуль $\mathcal{U}(M^*)_\chi$ с W -подмодулем в $\bigoplus_{j,i}(A_{\text{cris}})_{(r_j,i)}$, состоящим из наборов $(u_{\chi,(j,i)}^*)$ таких, что

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

(здесь w_{j_χ} пробегает элементы $W(\mathbb{F}_q)$). Этот модуль также порожден N/h_{j_χ} элементами

$$u_\chi^{*(i_0)} = (u_{(j,i)}^{(j_\chi, i_0)})_{\substack{1 \leq j \leq m \\ i \in \mathbb{Z}/N\mathbb{Z}}},$$

где $i_0 \in \mathbb{Z}/N\mathbb{Z}$ таков, что $i_0 \bmod h_{j_\chi} = i_\chi$.

Используем описание эпиморфизма $\mathcal{U}(i_{M,M^*})_\chi: \mathcal{U}(M^*)_\chi \rightarrow \mathcal{U}(M)_\chi$ из п. 3.2. Мы получим образующие $u_\chi^{(i_0)}$ для W -модуля $(\kappa_W \mathcal{U}(M))_\chi$ в виде

$$u_\chi^{(i_0)} = (u_{r,\chi}^{(i_0)})_{r \in S} \in \bigoplus_{r \in S} (A_{\text{cris}})_r,$$

где $i_0 \in \mathbb{Z}/N\mathbb{Z}$ и $i_0 \bmod h_{j_\chi} = i_\chi$, а для любого $r \in S$

$$u_{r,\chi}^{(i_0)} = \sum_{r_j(i)=r} u_{(j,i)}^{(j_\chi, i_0)}. \quad (4)$$

3.7. Пусть $1 \leq j_0 \leq m$ и $\tau \in \Gamma$. Тогда для любого $i \in \mathbb{Z}/N\mathbb{Z}$ имеем

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

где $w_{(j_0),\tau} \in W(\mathbb{F}_q)^*$ (см. п. 3.4).

Следующая лемма может быть легко доказана индукцией по $s \geq 0$.

ЛЕММА. Для $1 \leq j_0, j_1, \dots, j_s, \dots \leq m$, $a_0, b_1, \dots, a_{s-1}, b_s, \dots \in \mathbb{Z}/N\mathbb{Z}$ и $\tau \in \Gamma$ существуют $w_{(j_s, b_s; \dots; a_0, j_0), \tau} \in W(\mathbb{F}_q)$ такие, что:

1) для любого $i \in \mathbb{Z}/N\mathbb{Z}$ имеем

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

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

ЗАМЕЧАНИЕ. Как и в п. 3.6, если $w \in W(\mathbb{F}_q)$, то мы используем обозначение

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

Положим

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

где сумма берется по всем наборам $(j_s, b_s; \dots; a_0, j_0)$ таким, что $j_s = j$ и $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

В этих обозначениях сформулированная выше лемма дает следующее утверждение.

ПРЕДЛОЖЕНИЕ. Для произвольных $1 \leq j_0, j \leq m$, $i_0, i \in \mathbb{Z}/N\mathbb{Z}$ и $\tau \in \Gamma$ мы имеем

$$\tau u_{(j,i)}^{(j_0,i_0)} = \sum_{\substack{1 \leq j_1 \leq m \\ i_1 \in \mathbb{Z}/N\mathbb{Z}}} \sigma^{i_1}(w_{(j_1,i_1),\tau}^{(j_0,i_0)}) u_{(j,i)}^{(j_1,i_1)}, \quad (5)$$

$$v_p(w_{(j,i),\tau}^{(j_0,i_0)}) \geq A_{(j,i)}^{(j_0,i_0)}, \quad (6)$$

где $A_{(j,i)}^{(j_0,i_0)}$ – минимальное значение сумм

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

$j_s, b_s, a_{s-1}, \dots, b_1, a_0$ пробегают $\mathbb{Z}/N\mathbb{Z}$ при ограничениях $j_s = j$ и $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

Пусть $u_\chi^{(i_0)}$ – образующие для $(\kappa_W \mathcal{U}(M))_\chi$, построенные в п. 3.6. Тогда формула (4) из п. 3.6 дает следующее утверждение.

СЛЕДСТВИЕ. Для любого $\tau \in \Gamma$, характера χ группы $s(\Gamma_{\text{tr}})$ такого, что $r(\chi) = r_{j_\chi}(i_\chi)$, и $i_0 \in \mathbb{Z}/N\mathbb{Z}$ имеется следующее равенство:

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

где χ_1 пробегает все характеры группы $s(\Gamma_{\text{tr}})$ такие, что $r(\chi_1) \in S$, а i_1 пробегает элементы $\mathbb{Z}/N\mathbb{Z}$ такие, что $r_{j_{\chi_1}}(i_1) = r(\chi_1)$.

3.8. Рассмотрим функцию $n = n_U: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ для $\mathbb{Z}_p[\Gamma]$ -модуля $U = \mathcal{U}(M)$, определенную в п. 1.3 (мы используем естественное отождествление характеров группы H_1 с характерами группы $s(\Gamma_{\text{tr}})$).

Пусть $n_M: S \times S \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$ – функция из п. 2.3.

ПРЕДЛОЖЕНИЕ. Для любых $r, r_0 \in S$ имеется неравенство

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

ДОКАЗАТЕЛЬСТВО. Если $r = r_0$, то по определению мы имеем

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

Так как $n_M^*(r, r) = \infty$, мы имеем также

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

Таким образом, достаточно доказать наше предложение в случае $r \neq r_0$.

Если $r = r_j(i)$, $r_0 = r_{j_0}(i_0)$, где $1 \leq j, j_0 \leq m$, $i, i_0 \in \mathbb{Z}/N\mathbb{Z}$, то следствие п. 3.7 дает

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

Теперь из предложения п. 3.7 следует, что значение $n_U(r_0, r)$ не меньше чем минимальное значение выражения

$$n_M^*(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) + \dots + n_M^*(r_{j_0}(a_0), r_{j_1}(b_1)), \quad (7)$$

где $(j_s, b_s; \dots; a_0, j_0)$ – произвольный набор такой, что $j_s = j$ и $i - i_0 = b_s - a_{s-1} + \dots + b_1 - a_0$.

Допустим, что набор $(j_s, b_s; \dots; a_0, j_0)$ с описанными выше ограничениями дает минимальное значение суммы (7). Тогда из свойства $n_M^*(r_1(1), r_2(1)) = n_M^*(r_1, r_2)$ вытекают следующие равенства:

$$\begin{aligned} n_M^*(r_{j_{s-1}}(a_{s-1}), r_{j_s}(b_s)) &= n_M^*(r^{(1)}, r), \\ n_M^*(r_{j_{s-2}}(a_{s-2}), r_{j_{s-1}}(b_{s-1})) &= n_M^*(r^{(2)}, r^{(1)}), \\ &\dots \\ n_M^*(r_{j_0}(a_0), r_{j_1}(b_1)) &= n_M^*(r^{(s)}, r^{(s-1)}), \end{aligned}$$

где

$$\begin{aligned} r^{(1)} &= r_{j_{s-1}}(i + a_{s-1} - b_s), \\ r^{(2)} &= r_{j_{s-2}}(i + a_{s-2} + a_{s-1} - b_{s-1} - b_s), \\ &\dots \\ r^{(s-1)} &= r_{j_1}(i + a_1 + \dots + a_{s-2} - b_2 - \dots - b_{s-1}), \\ r^{(s)} &= r_{j_0}(i + a_0 + \dots + a_{s-1} - b_1 - \dots - b_s) = r_{j_0}(i_0) = r_0. \end{aligned}$$

Следовательно,

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

согласно определению функции n_M . Предложение доказано.

3.9. Рассмотрим граф $v_M \in \mathcal{V}_S$ функции n_M (см п. 2.4).

Предположим, что $(r^0, r^1) \in S_{v_M} \subset S \times S$. Очевидно, $r^0 \neq r^1$. По определению отображения $\pi: \Phi_S \rightarrow \mathcal{V}_S$ мы имеем $v_M(r^0, r^1) = n_M(r^0, r^1)$ и, очевидно,

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

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

Обозначим через j^0, j^1 однозначно определенные индексы из $[1, m]$ такие, что $r_{j^0} \in S(r^0)$ и $r_{j^1} \in S(r^0)$.

Рассмотрим фильтрованный модуль $M(r^1, r^0) \in \text{MF}_f$ такой, что:

а) $M(r^1, r^0)$ – свободный W -модуль с базисом

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

б) для $0 \leq l < p$ подмодуль фильтрации $M(r^1, r^0)^l$ порожден элементами множества

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

с) σ -линейные морфизмы ϕ_l , $0 \leq l < p$, определены (однозначно) условиями

$$\begin{aligned} \phi_{l_0(r(-1))} m_{r(-1)}^0 &= m_r^0, \quad r \in S(r^0), \\ \phi_{l_0(r(-1))} m_{r(-1)}^1 &= m_r^1 + \sum_{(r', r) \in S_{(r^0, r^1)}} \beta_{rr'}^* m_{r'}^0, \quad r \in S(r^1), \end{aligned}$$

где

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

$\beta_{rr'}^* = p^{-v_M(r^0, r^1)} \beta_{rr'}$, если $(r', r) \in S_{(r^0, r^1)}$, и $\beta_{rr'}^* = 0$ в противном случае.

3.10. Пусть χ^1, χ^0 – характеры группы Γ_{tr} такие, что $r(\chi^1) = r^1$ и $r(\chi^0) = r^0$. Очевидно, что $\chi^1 \neq \chi^0$.

ПРЕДЛОЖЕНИЕ. *Относительно обозначений и предположений пп. 3.7–3.9 следующие условия эквивалентны:*

а) $n_U(r^0, r^1) \leq v_M(r^0, r^1)$;

б) существуют $u \in \mathcal{U}(M(r^1, r^0))$ и $\tau_0 \in \Gamma$ такие, что

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

с) для некоторых $w_0 \in W(\mathbb{F}_q)$ и $\tau_0 \in \Gamma$ выполнено

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

где сумма берется по всем $i^0, i^1, b_1, a_0 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $i^1 - i^0 = b_1 - a_0$, $r_{j^0}(i^0) = r^0$ и $r_{j^1}(i^1) = r^1$.

ДОКАЗАТЕЛЬСТВО. Докажем эквивалентность условий а) и с). Условие а) эквивалентно существованию $u \in U = \mathcal{U}(M)$ и $\tau_0 \in \Gamma$ таких, что

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

В обозначениях п. 3.6 этот факт эквивалентен существованию

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

такого, что образ $(\tau_0 u_{\chi^0}^*)_{\chi^1}$ в U_{χ^1} не принадлежит $p^{v_M(r^0, r^1)+1} U_{\chi^1}$.

В обозначениях пп. 3.6, 3.7 имеются следующие свойства:

1) $u_{\chi^0}^* = (u_{\chi^0, (j, i)}^*)$, где

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

а суммирование ведется по всем $i^0 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $r_{j^0}(i^0) = r^0$;

2) $\tau_0 u_{\chi^0}^* = (\tau_0 u_{\chi^0, (j, i)}^*)$, где

$$\tau_0 u_{\chi^0, (j, i)}^* = \sum_{i^0, j_1, i_1} \sigma^{i^0}(w_{j_0}) \sigma^{i_1}(w_{(j_1, i_1), \tau_0}^{(j^0, i^0)}) u_{(j, i)}^{(j_1, i_1)},$$

а суммирование ведется по всем $1 \leq j_1 \leq m$, $i_1 \in \mathbb{Z}/N\mathbb{Z}$ и всем $i^0 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $r_{j^0}(i^0) = r^0$;

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

$$u_{\chi^0, \chi^1, (j, i)}^* = \sum_{i^0, i^1} \sigma^{i^0}(w_{j_0}) \sigma^{i^1}(w_{(j^1, i^1), \tau_0}^{(j^0, i^0)}) u_{(j, i)}^{(j^1, i^1)},$$

а суммирование ведется по всем $i^0, i^1 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $r_{j^0}(i^0) = r^0$ и $r_{j^1}(i^1) = r^1$.

Пусть $w_{(j_s, b_s; \dots; a_0, j_0), \tau_0}$ – некоторое слагаемое выражения для $w_{(j^1, i^1), \tau_0}^{(j^0, i^0)}$ из п. 3.7. Из того, что $(r^0, r^1) \in S_{v_M}$, и согласно части 2) леммы п. 3.7 получаем

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

а если $s \geq 2$, то

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

Следовательно,

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

Из свойства $n_M(r, r) \geq 1$ и из построения элементов $u_{(j, i)}^{(j^1, i^1)}$ вытекает, что

$$u_{(j^1, i)}^{(j^1, i^1)} \equiv u(i, j^1) \delta(i, i^1) \mod p A_{\text{cris}}.$$

По этим причинам из свойства 3) следует, что

$$\begin{aligned} u_{\chi^0, \chi^1, (j^1, i)}^* &\equiv \sum_{i^0, i^1, b_1, a_0} \sigma^{i^0}(w_{j^0}) \sigma^{i^1}(w_{(j^1, b_1; a_0, j^0), \tau_0}) \\ &\quad \times u(i, j^1) \delta(i, i^1) \mod p^{v_M(r^0, r^1)+1} A_{\text{cris}}, \end{aligned}$$

где сумма берется по всем $i^0, i^1, b_1, a_0 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $i^1 - i^0 = b_1 - a_0$, $r_{j^0}(i^0) = r^0$ и $r_{j^1}(i^1) = r^1$.

Используем формулы п. 3.2 для доказательства того, что значение $m_r \in M$ на образе $(\tau_0 u_{\chi^0}^*)_{\chi^1}$ в $\mathcal{U}(M)_{\chi^1}$ равняется нулю при $r \neq r^1$ и совпадает с выражением из части с) нашего предложения при $r = r^1$. Таким образом, а) и с) эквивалентны.

Докажем эквивалентность условий в) и с). Рассмотрим элементы

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

из п. 3.5. Повторяя рассуждения из п. 3.6, мы получаем следующее описание элементов Γ -модуля $\mathcal{U}(M(r^0, r^1))$.

Для любого $u \in \mathcal{U}(M(r^1, r^0))$ существуют $w_0, w_1 \in W(\mathbb{F}_q)$ такие, что:

– если $r \in S(r^0)$, то

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

– если $r \in S(r^1)$, то

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

где последняя сумма берется по всем $i, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $r_{j^1}(i) = r$ и $(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}$.

Для χ^0 -компоненты u_{χ^0} точки u мы имеем:

– если $r \in S(r^0)$, то

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

– если $r \in S(r^1)$, то

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

где последняя сумма берется по всем $i^0, i, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $i^0 = i - b_1 + a_0$, $r_{j^0}(i^0) = r^0$, $r_{j^1}(i) = r$ и $(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}$.

Теперь мы можем использовать то, что $\chi^0 \neq \chi^1$ и

$$\begin{aligned} \tau_0 u^*(i, j^1, b_1; a_0, j^0) &= \sigma^{i-b_1+a_0}(w_{(j^0), \tau_0}) u^*(i, j^1, b_1; a_0, j^0) \\ &\quad + \sigma^i(w_{(j^1, b_1; a_0, j^0), \tau_0}^*) u(i, j^1), \end{aligned}$$

где $\tau_0 \in \Gamma$ и

$$w_{(j^1, b_1; a_0, j^0), \tau_0}^* = p^{-n_M^*(r^0, r^1)} w_{(j^1, b_1; a_0, j^0), \tau_0}, \quad (8)$$

чтобы получить следующее описание точки $(\tau_0 u_{\chi^0})_{\chi^1}$:

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

$$m_r^1((\tau_0 u_{\chi^0})_{\chi^1}) = \delta(r, r^1) \sum_{i^0, i^1, a_0, b_1} \sigma^{i^0}(w_0) \sigma^{i^1}(w_{(j^1, b_1; a_0, j^0), \tau_0}^*) u(i^1, j^1), \quad (9)$$

где сумма берется по всем $i^0, i^1, a_0, b_1 \in \mathbb{Z}/N\mathbb{Z}$ таким, что $i^0 = i^1 - b_1 + a_0$, $r_{j^0}(i^0) = r^0$, $r_{j^1}(i^1) = r^1$ (мы используем то, что условие $(r_{j^0}(a_0), r_{j^1}(b_1)) \in S_{(r^0, r^1)}$ является теперь следствием других условий, так как $r_{j^1}(b_1) = r^1(b_1 - i^1)$, $r_{j^0}(a_0) = r^0(a_0 - i^0)$ и $b_1 - i^1 = a_0 - i^0$).

Таким образом, утверждение б) нашего предложения эквивалентно существованию $w_0 \in W(\mathbb{F}_q)$ и $\tau_0 \in \Gamma$ таких, что правая часть формулы (9) не принадлежит pA_{cris} для $r = r^1$. Но это эквивалентно утверждению части с) нашего предложения благодаря соотношению (8). Предложение доказано.

3.11. Используем обозначения и предположения из п. 3.9.

ПРЕДЛОЖЕНИЕ. *Эквивалентные утверждения а)–с) предложения 3.10 являются справедливыми.*

Очевидно, из этого предложения (нам нужна часть а) предложения 3.10), а также из предложений шп. 3.8 и 2.4.3 вытекает утверждение теоремы А.

ДОКАЗАТЕЛЬСТВО. Достаточно доказать утверждение б) предложения 3.10. Это утверждение использует только структуру $\mathbb{F}_p[\Gamma]$ -модуля $\mathcal{U}(M(r^1, r^0)) \otimes_{\mathbb{F}_p} U_1(r^1, r^0)$. Модули Галуа такого типа были детально изучены (в качестве важного шага при описании всех аннулируемых умножением на p подфакторов модулей Фонтена–Лаффе) в работе [2]. По этой причине мы дадим лишь набросок доказательства этого предложения.

3.11.1. В категории MF имеется естественная точная последовательность

$$0 \longrightarrow M(r^0) \longrightarrow M(r^1, r^0) \otimes k \longrightarrow M(r^1) \longrightarrow 0, \quad (10)$$

где $M(r^1)$, $M(r^0)$ являются простыми объектами категории MF (см. п. 2.1). Это дает точную последовательность $\mathbb{F}_p[\Gamma]$ -модулей

$$0 \longrightarrow H^1 \longrightarrow U_1(r^1, r^0) \longrightarrow H^0 \longrightarrow 0, \quad (11)$$

где H^1 и H^0 – простые $\mathbb{F}_p[\Gamma]$ -модули с множествами характеров $S(r^1)$ и $S(r^0)$ соответственно. Расширение (11) не является тривиальным, так как расширение (10) – нетривиальное расширение в категории MF, а функтор U является вполне строгим на категории MF($p - 2$).

Класс эквивалентности расширений (11) задается ненулевым элементом $e(r^1, r^0)$ группы

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

(здесь I – подгруппа высшего ветвления в Γ).

Утверждение б) предложения 3.10 означает, что (χ^0, χ^1) -компонента

$$e(r^1, r^0)_{\chi^0, \chi^1} \in \text{Hom}^{\Gamma_{\text{tr}}}(I, \text{Hom}(H_{\chi^0}^0, H_{\chi^1}^1))$$

элемента $e(r^1, r^0)$ не является тривиальной.

3.11.2. Для любого $r \in R'_p \setminus \{0\} = \{r \in \mathbb{Q} \cap (0, 1) \mid v_p(r) \geq 0\}$ определим подполе $K(r)$ в $\overline{K}$ следующим образом. Поле $K(r)$ является композитом полей

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

где $T_\beta^p - T_\beta = \beta \theta_b^{-a}$, $r = a/b$, $a, b \in \mathbb{Z}_{\geq 0}$, $v_p(b) = 0$ и $\theta_b \in K_{\text{tr}}$ таков, что $\theta_b^b = p$.

Мы имеем следующие свойства:

- а) $K(r)/K$ – расширение Галуа;
- б) $I(r) = \text{Gal}(K(r)/K_{\text{tr}})$ – абелева группа периода p ;
- в) $I(r)$ – изотипический $\mathbb{F}_p[\Gamma_{\text{tr}}]$ -модуль, где действие группы Γ_{tr} задается множеством характеров, сопряженных характеру χ такому, что $r(\chi^{-1}) = r$;
- г) если $r = l/(p^{N_1} - 1)$ для некоторых $N_1 \in \mathbb{N}$ и $l \in \mathbb{N}$, то $K(r)$ совпадает с композитом полей из множества

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

где $T_{\beta, N_1}^{p^{N_1}} - T_{\beta, N_1} = \beta \pi_{N_1}^{-l}$ и $\pi_{N_1}^{p^{N_1}-1} = -p$.

3.11.3. Используем явную конструкцию ограничения функтора Фонтена–Лаффе на подкатегорию $\text{MF}_1(p-2)$ (см. конец п. 2.2). Элементы модуля Галуа $U_1(r^1, r^0)$ могут быть отождествлены с вычетами по модулю $p\overline{O}$ решений

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

в $\overline{K}$ следующей системы уравнений:

$$\begin{aligned} \left(-\frac{1}{p}\right)^{l_0(r(-1))} X_{r(-1)}^p &= X_r, \quad r \in S(r^0), \\ \left(-\frac{1}{p}\right)^{l_0(r(-1))} Y_{r(-1)}^p &= Y_r + \sum_{(r', r) \in S_{(r^0, r^1)}} \sigma^{-1}(\beta_{rr'}^*) X_{r'}, \quad r \in S(r^1). \end{aligned}$$

Над полем K_{tr} все решения этой системы могут быть выражены через решения уравнений

$$T^q - T = \sigma^{-1}(\beta_{rr'}^*)\pi_N^{l-l'},$$

где $N \in \mathbb{N}$, $q = p^N$, $\pi_N^{q-1} = -p$, $r = l/(q-1)$, $r' = l'/(q-1)$ и $(r', r) \in S_{(r^0, r^1)}$.

Теперь свойство d) из п. 3.11.2 дает, что все точки $\mathbb{F}_p[\Gamma]$ -модуля $U_1(r^1, r^0)$ определены над композитом полей $K(r' - r)$, где

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

3.11.4. Возьмем $\chi_0 \in S(r^0)$, $\chi_1 \in S(r^1)$ так, чтобы $e(r^1, r^0)_{\chi_0, \chi_1} \neq 0$ (такие χ_0 и χ_1 существуют, так как $e(r^1, r^0) \neq 0$). Мы должны доказать, что

$$(r(\chi_0), r(\chi_1)) \in S_{(r^0, r^1)},$$

так как тогда ввиду условия сопряженности $e(r^1, r^0)_{\chi^0, \chi^1} \neq 0$, и предложение доказано. Согласно п. 3.4.3 мы имеем

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

Существует $(\tilde{r}', \tilde{r}) \in S_{(r^0, r^1)}$ такой, что проекция $e(r^1, r^0)_{\chi_0, \chi_1}$ на

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

не является нулевой. Следовательно, характер $\chi_0^{-1}\chi_1$ действует нетривиально на $I(\tilde{r}' - \tilde{r})$, и отсюда вытекает, что для некоторого $i \in \mathbb{Z}$ мы имеем $r(\sigma^i(\chi_0^{-1}\chi_1)) = \tilde{r}' - \tilde{r}$. Это дает

$$r(\chi_0)(i) - r(\chi_1)(i) \equiv \tilde{r}' - \tilde{r} \pmod{\mathbb{Z}}.$$

Очевидно, $(\tilde{r}', \tilde{r}) \in S_{(r^0, r^1)}$ влечет $\tilde{r}' \neq \tilde{r}$, и согласно предположению С4 об элементах множества S мы имеем $\tilde{r}' = r(\chi_0)(i)$ и $\tilde{r} = r(\chi_1)(i)$, т.е. $(r(\chi_0), r(\chi_1)) \in S_{(\tilde{r}', \tilde{r})} = S_{(r^0, r^1)}$. Предложение и теорема А доказаны.

3.12. Случай “максимального тора”. Предположим, что множество S удовлетворяет условию С3 из §1, т.е. $S = \{r, \dots, r(h-1)\}$, где $h = h(r)$. В этом случае функция n_U принимает значения в $\mathbb{N} \cup \{\infty\}$, и мы можем использовать ее аналог

$$n_{U, \chi}: \mathbb{Z}/h\mathbb{Z} \longrightarrow \mathbb{N} \cup \{\infty\}$$

из п. 1.4 (где $\chi \in \text{Char } \Gamma_{\text{tr}}$ таков, что $r(\chi) = r$).

Рассмотрим следующее свойство множества S .

С5. $(l_1(r)X^{p^{h-1}} + \dots + l_h(r)X) \pmod{p}$ и $X^{p^h-1} - 1 \pmod{p}$ являются взаимно простыми элементами кольца многочленов $\mathbb{F}_p[X]$.

ПРЕДЛОЖЕНИЕ. Если множество S удовлетворяет дополнительному условию С5, то образ G подгруппы высшего ветвления I группы Галуа Γ содержит “максимальный тор” $1 + pE^0$ (напомним, что $E = \text{End}_{\mathbb{Z}_p} U$ с естественной структурой $s(\Gamma_{\text{tr}})$ -модуля и $E^0 = E^{s(\Gamma_{\text{tr}})}$).

ДОКАЗАТЕЛЬСТВО. Соотнесем сначала общую конструкцию, использованную при доказательстве теоремы А, с нашей специальной ситуацией. Мы имеем $m = 1$, $h_1 = h = N$, $M = M^*$, $q = p^h$ и $S = \{r, \dots, r(h-1)\}$.

Если χ – характер группы Γ_{tr} такой, что $r(\chi) = r$, то U_χ порожден элементом $u_\chi^{(0)}$; для любого $\tau \in \Gamma$ мы имеем

$$\tau u_\chi^{(0)} = \sum_{i_1 \in \mathbb{Z}/h\mathbb{Z}} \sigma^{i_1} (w_{(1,i_1),\tau}^{(1,0)}) u_{\chi_1}^{(i_1)},$$

где $r(\chi_1) = r(i_1)$ и $w_{(1,i_1),\tau}^{(1,0)} \in W(\mathbb{F}_q)$ (см. п. 3.7). Так как $n_{U,\chi}(0) \geq 2$, мы имеем для произвольного $\tau \in \Gamma$

$$w_{(1,0),\tau}^{(1,0)} \equiv w_{(1),\tau} \pmod{p^2 W(\mathbb{F}_q)},$$

где

$$w_{(1),\tau} = \eta_{LT}(\tau) l_0(r) + l_1(r) \sigma^{-1} + \dots + l_{h-1}(r) \sigma^{-h+1}$$

(см. пп. 3.4 и 3.7).

Следовательно, множество $\left\{ \frac{w_{(1),\tau} - 1}{p} \pmod{p} \mid \tau \in I \right\}$ совпадает с образом $\mathbb{F}_q$ при $\mathbb{F}_p$ -линейном эндоморфизме R , который задается с помощью соответствия

$$R: \alpha \mapsto l_0(r)\alpha + l_1(r)\sigma^{-1}\alpha + \dots + l_{h-1}(r)\sigma^{-h+1}(\alpha).$$

Из предположения С5 вытекает, что $\text{Ker } R = 0$ и, следовательно, $\text{Im } R = \mathbb{F}_q$. Это дает

$$G \pmod{p^2 E} \supset 1 + pE^0 \pmod{p^2 E},$$

что, очевидно, эквивалентно утверждению нашего предложения.

СЛЕДСТВИЕ. При дополнительном предположении С5 образ группы Галуа Γ в $\text{Aut}_{\mathbb{Z}_p} U$ полностью определяется функцией $n_U \in \mathcal{F}_{S_U}$.

Список литературы

1. Абрашкин В. А. Модификация функтора Фонтена–Лаффе // Изв. АН СССР. Сер. матем. 1989. Т. 34. №3. С. 451–497.
2. Абрашкин В. А. Модулярные представления группы Галуа локального поля и обобщение гипотезы Шафаревича // Изв. АН СССР. 1989. Т. 35. №3.
3. Бенуа Д. Г. О p -адических представлениях, возникающих из формальных групп // Тр. С.-Петербург. матем. об-ва. 1995. Т. 3. С. 135–139.
4. Бенуа Д. Г., Востоков С. В. Норменное спаривание в формальных группах и представления Галуа // Алгебра и анализ. 1990. Т. 2. №6. С. 69–97.
5. Fontaine J.-M. Points d'ordre fini d'un groupe formel sur une extension non ramifie de $\mathbb{Z}_p$ // Bull. Soc. math. France. 1974. Memoire 37. P. 75–79.
6. Fontaine J.-M. Groupes p -divisibles sur les corps locaux // Asterisque. V. 47–48. Paris: Soc. Math. de France, 1977.
7. Fontaine J.-M., Laffaille G. Construction de representations p -адических // Ann. Sci. E.N.S. 1982. Ser.15. № 4. P. 547–608.
8. Nakamura T. On torsion points of formal groups over a ring of Witt vectors // Math. Z. 1986. V. 193. P. 397–404.
9. Wintenberger J.-P. Un scindage de la filtration de Hodge pour certaines varietes algebriques sur le corps locaux // Annals of Math. 1984. V. 119. P. 511–548.