Записки научных
семинаров ПОМИ
Том 430, 2014 г.

С. В. Востоков, И. И. Некрасов

ФОРМАЛЬНЫЙ МОДУЛЬ ЛЮБИНА – ТЕЙТА В ЦИКЛИЧЕСКОМ НЕРАЗВЕТВЛЕННОМ p – РАСШИРЕНИИ КАК МОДУЛЬ ГАЛУА

§1. Введение

Пусть M/L, L/K, $K/\mathbb{Q}_p$ – произвольные конечные расширения Галуа, где p – фиксированное простое число, а F – формальный групповой закон Любина–Тейта над кольцом $\mathcal{O}_K$ для простого элемента π. Тогда максимальный простой идеал $\mathfrak{m}_M$ поля M допускает естественную структуру $\mathcal{O}_K[G]$-модуля.

$$\mathbb{Q}_p \;\text{——}\; K \;\text{——}\; L \overset{G}{\text{——}} M$$

Классической ситуацией является случай, когда K совпадает с $\mathbb{Q}_p$ и $F = F_m$ – мультипликативный закон. Этот случай рассмотрен достаточно подробно в цикле работ К. Ивасава [1, 2], М. Краснера [3], З. И. Боревича и С. В. Востокова [5–8].

Как и в классическом случае, на строение $\mathcal{O}_K[G]$-модуля $F(\mathfrak{m}_M)$ влияют следущие факторы:

- являются ли поля L и M регулярными или нет, то есть содержат ли данные поля корни изогении $\mathrm{Ker}[\pi]$,
- ветвление расширения M/L.

В данной работе рассматривается случай неразветвленного циклического p-расширения M/L и поля M и L имеют степень иррегулярности $s \geqslant 1$, то есть в M и L содержится первообразный корень $\mathrm{Ker}[\pi^s]$, но не содержится образующей $\mathrm{Ker}[\pi^{s+1}]$.

Условимся в следующих обозначаниях:

n – степень поля L над K;

p^m – порядок группы $G = \mathrm{Gal}(M/L)$;

σ – образующая G;

$\zeta = \zeta_s$ – образующая $\mathrm{Ker}[\pi^s]$, содержащаяся в L;

Ключевые слова: формальный модуль Любина–Тейта, модуль Галуа, локальное поле.

Работа поддержана грантом РФФИ номер 14-01-00393 а.

$\overline{K}$, $\overline{L}$, $\overline{M}$ – поля вычетов K, L и M соответственно;
$x +_F y := F(x, y)$.

§2. Леммы

Известна следующая лемма [9, предложение 2.3].

Лемма 1. *Для любого натурального k модуль $\mathrm{Ker}[\pi^k]_F$ является циклическим $\mathcal{O}_K$-модулем, изоморфным $\mathcal{O}_K/\pi^k\mathcal{O}_K$.*

Лемма 2. *Если $\theta_1,\ldots,\theta_k$ являются образующими для $F(\mathfrak{m}_M)/[\pi](F(\mathfrak{m}_M))$ как векторного пространства над $\overline{K}$, то $\theta_1,\ldots,\theta_k$ – образующие для $\mathcal{O}_K$-модуля $F(\mathfrak{m}_M)$.*

Доказательство. Покажем, что $\theta_1, \ldots, \theta_k$ порождают $F(\mathfrak{m}_M)$.

Пусть $\eta = \eta_0 \in F(\mathfrak{m}_M)$. Тогда по предположению существуют[1] $a_1^0, \ldots, a_k^0 \in \overline{K}$ такие, что верно равенство:

$$\eta_0 = \sum_{i=1}^{k} {}_F[a_i^0](\theta_i) +_F [\pi](\eta_1).$$

Аналогично, по предположению существуют $a_1^1, \ldots, a_k^1 \in \overline{K}$ такие, что

$$\begin{aligned}
\eta_0 &= \sum_{i=1}^{k} {}_F[a_i^0](\theta_i) +_F [\pi] \left(\sum_{i=1}^{k} {}_F[a_i^1](\theta_i) +_F [\pi](\eta_2) \right) \\
&= \sum_{i=1}^{k} {}_F[a_i^0](\theta_i) +_F \sum_{i=1}^{k} {}_F[a_i^1\,\pi](\theta_i) +_F [\pi^2](\eta_2) \\
&= \sum_{i=1}^{k} {}_F[a_i^0 + a_i^1\pi](\theta_i) +_F [\pi^2](\eta_2).
\end{aligned}$$

Продолжая процесс, получим

$$\eta = \sum_{i=1}^{k} {}_F[\alpha_i](\theta_i)\,,$$

где $\alpha_i = \sum_{j=1}^{\infty} a_i^j\,\pi^j \in \mathcal{O}_K$. $\square$

---

[1]На самом деле $a_i^j \in \mathcal{R}_K$ – представители Тейхмюллера, но имеется биекция $\overline{K} \leftrightarrow \mathcal{R}_K \subset K$.

Лемма 3. а) *Если нормы $N_{F(\mathfrak{m}_M)}(\alpha_j)$ элементов α_j $(1 \leqslant j \leqslant k)$ из $F(\mathfrak{m}_M)$ линейно независимы в $F(\mathfrak{m}_M)/[\pi]F(\mathfrak{m}_M)$, то линейно независимы в $F(\mathfrak{m}_M)/[\pi]F(\mathfrak{m}_M)$ и элементы*

$$\alpha_j^{\sigma^i} \ (1 \leqslant j \leqslant k, 0 \leqslant i \leq p^m).$$

б) *Если элементы γ, $N_{F(\mathfrak{m}_M)}(\alpha_j)$ при $(1 \leqslant j \leqslant k)$, где $\gamma \in F(\mathfrak{m}_L)$, линейно независимы в $F(\mathfrak{m}_M)/[\pi]F(\mathfrak{m}_M)$, то*

$$\gamma, \quad \alpha_j^{\sigma^i} \ (1 \leqslant j \leqslant k, 0 \leqslant i \leq p^m)$$

линейно независимы в $F(\mathfrak{m}_M)/[\pi]F(\mathfrak{m}_M)$.

Доказательство. а) Рассмотрим оператор $\Gamma := \sigma -_F 1$. Тогда

$$\underbrace{\Gamma \circ \Gamma \circ \cdots \circ \Gamma}_{p^m \text{ штук}} = \Gamma^{p^m} \equiv 0 \,(\mathrm{mod}\, p),$$

$$\Gamma^{p^m-1} \equiv 1 +_F \sigma +_F \cdots +_F \sigma^{p^m-1} \equiv N_{F(\mathfrak{m}_M)} \,(\mathrm{mod}\, p).$$

Оба сравнения являются следствием того, что $|G| = p^m$.

Теперь предположим противное, а именно, что имеет место соотношение:

$$\sum_{i,j} {}_F \Gamma^i([a_{ij}](\alpha_j)) \equiv 1 \,(\mathrm{mod}\, [\pi](F(\mathfrak{m}_M))), \qquad (*)$$

где не все $a_{ij} \,\vdots\, \pi$. Тогда пусть i_0 – минимальный индекс такой, что существует j: $a_{i_0 j} \not\equiv 0 \,(\mathrm{mod}\, \pi)$. Подействуем оператором $\Gamma^{p^m - i_0 - 1}$ на соотношение зависимости элементов $(*)$ и получим:

$$\sum_{j} {}_F [a_{i_0 j}](N_{F(\mathfrak{m}_M)}) \equiv 1 \,(\mathrm{mod}\, [\pi](F(\mathfrak{m}_M))).$$

Последнее сравнение приводит к противоречию с независимостью норм. То есть линейно независимыми являются $\{\Gamma^i(\alpha_j)\}_{i,j}$. Откуда следует требуемое утверждение, так как $\{\Gamma^i(\alpha_j)\}_{i,j}$ и $\{\sigma^i(\alpha_j)\}_{i,j}$ связаны невырожденным линейным преобразованием.

б) С учётом того, что $\sigma^i(\gamma) = \gamma$, рассуждения из первого пункта доказывают требуемое. □

Лемма 4. *Естественный гомоморфизм*

$$F(\mathfrak{m}_L)/[\pi](F(\mathfrak{m}_L)) \to F(\mathfrak{m}_M)/[\pi]F(\mathfrak{m}_M)$$

имеет нетривиальное ядро тогда и только тогда, когда

$$\zeta_1 \in (\sigma -_F \ 1)(F(\mathfrak{m}_M)).$$

Доказательство. Если $\eta \in F(\mathfrak{m}_L)\backslash[\pi]F(\mathfrak{m}_L)$ и при этом выполнено $\eta = [\pi](\delta)$, где $\delta \in F(\mathfrak{m}_M)$, то $(\sigma -_F 1)(\delta) \neq 0$ и $[\pi]((\sigma -_F 1)(\delta)) = 0$.

Если же $\zeta_1 = (\sigma -_F 1)(\eta)$, то $\eta \in F(\mathfrak{m}_M)\backslash F(\mathfrak{m}_L)$ и $[\pi](\eta) \in F(\mathfrak{m}_L)$. □

Лемма 5. *Если M/L неразветвлено, то $H^1(G,\, F(\mathfrak{m}_M))$ тривиальна.*

Доказательство. Имеется короткая точная последовательность G-модулей:

$$0 \to F(\mathfrak{m}_M^2) \to F(\mathfrak{m}_M) \to \mathbb{F}_{r^l} \to 0,$$

где $r = |\overline{L}|$ и $r^l = |\overline{M}|$ ($l = p^m$, так как M/L неразветвлено). Откуда получаем длинную точную последовательность:

$$\begin{aligned} 0 \to H^0(G, F(\mathfrak{m}_M^2)) &\to H^0(G, F(\mathfrak{m}_M)) \to H^0(G, \mathbb{F}_{r^l}) \\ \to H^1(G, F(\mathfrak{m}_M^2)) &\to H^1(G(F, \mathfrak{m}_M)) \to H^1(G, \mathbb{F}_{r^l}) \to \dots \end{aligned}$$

При этом $H^0(G, F(\mathfrak{m}_M^i)) = F(\mathfrak{m}_L^i)$ и $H^0(G, \mathbb{F}_{r^l}) = \mathbb{F}_r$, а потому $H^1(G, F(\mathfrak{m}_M^2))$ тривиальна. Поэтому, если для $x \in F(\mathfrak{m}_M)$ выполняется $N_{F(\mathfrak{m}_M)}(x) = 0$, применим $[\pi]$ к обеим частям и получим $[\pi](x) = \sigma(z) -_F z$ для некоторого $z \in F(\mathfrak{m}_M^2)$. Теперь найдём $t = t_1\pi_0 + \dots \in F(\mathfrak{m}_M)$ такой, что верно $z = [\pi](t)$, последовательно находя $t_0, t_1, \dots$.

Окончательно получим, что $x = \sigma(t) -_F t$, то есть $H^1(G,\, F(\mathfrak{m}_M))$ тривиальна. □

Лемма 6. *Если расширение M/L неразветвлено, то*

$$N_{F(\mathfrak{m}_M)}(F(\mathfrak{m}_M)) = F(\mathfrak{m}_L).$$

Доказательство. Пусть $\alpha = a_k \cdot \pi^k + \dots \in F(\mathfrak{m}_L)$. Будем искать $\beta = b_k \cdot \pi^k + \dots \in F(\mathfrak{m}_M)$ такое, что $\alpha = \beta +_F \sigma(\beta) +_F \dots +_F \sigma^{p^m-1}(\beta)$, последовательно находя $b_k,\, b_{k+1}, \dots$.

$$\begin{aligned} \beta +_F \sigma(\beta) +_F \dots +_F \sigma^{p^m-1}(\beta) &\equiv (b_k + \sigma(b_k) + \dots + \sigma^{p^m-1}(b_k)) \cdot \pi^k \\ &\equiv Tr_{M/L}(\beta) \equiv \alpha \,(\mathrm{mod}\ \pi^{k+1}). \end{aligned}$$

Но известно [4, теорема 5.1], что если M/L слабо разветвлено, то $Tr_{M/L}(\mathcal{O}_M) = \mathcal{O}_L$. Поэтому последовательно найдутся подходящие $b_k,\, b_{k+1}, \dots$. □

§3. Основная теорема

Теорема 1. *Пусть расширение M/L неразветвлено, поля M и L имеют одинаковый показатель иррегулярности s. Тогда для $\mathcal{O}_K[G]$-модуля $F(\mathfrak{m}_M)$ существует система образующих $\theta_1, \dots, \theta_{n-1}, \xi, \omega$ с единственным определяющим соотношением*

$$(\sigma -_F 1)(\omega) = [\pi^s](\xi).$$

Доказательство. Так как совпадают показатели иррегулярности у M и L, то $\zeta \notin [\pi](F(\mathfrak{m}_M))$. А значит в $F(\mathfrak{m}_L)$ можно выбрать единицы $\epsilon_1, \dots, \epsilon_{n-1}$ так, что $\epsilon_1, \dots, \epsilon_{n-1}, \zeta$ линейно независимы. Тогда пусть $\zeta = N_{F(\mathfrak{m}_M)}(\xi), \epsilon_j = N_{F(\mathfrak{m}_M)}(\theta_j)$. По лемме 3 система

$$\sigma^i(\theta_j),\, \sigma^i(\xi)\, (1 \leqslant j \leqslant n-1, 0 \leqslant i \leq p^m)$$

линейно независима в $F(\mathfrak{m}_L)/[\pi](F(\mathfrak{m}_L))$. Также из $N_{F(\mathfrak{m}_M)}([\pi^s]\xi) = 0$ и тривиальности $H^1(G, F(\mathfrak{m}_M))$ следует, что существует $\omega \in F(\mathfrak{m}_L)$ такое, что $(\sigma -_F 1)(\omega) = [\pi^s](\xi)$.

Покажем, что ω не является линейной комбинацией элементов $\sigma^i(\theta_j)$, $\sigma^i(\xi)$ в пространстве $F(\mathfrak{m}_M)/F(\mathfrak{m}_M)$.

Предположим противное. Тогда выполняется соотношение вида

$$\omega = (\sum_{i=1}^{n-1}{}_F [x_i](\epsilon_i)) +_F \zeta^x +_F [\pi](\beta),\ \beta \in F(\mathfrak{m}_M),$$

с $x_i \in \mathcal{O}_K$. Применяя к этому равенству оператор Γ, получим

$$[\pi^s](\xi) = [\pi]((\sigma -_F 1)(\beta)),$$

поэтому

$$[\pi^{s-1}](\xi) = (\sigma -_F 1)(\beta) \oplus [k](\zeta_1),$$

что после вычисления нормы даёт нам неверное равенство $[\pi^{s-1}](\zeta) = 0$. Этим доказана линейная независимость элементов $\{\sigma^i(\theta_j),\, \sigma^i(\xi)\}$.

По построению ясно, что единственным соотношением зависимости среди $\theta_1, \dots, \theta_{n-1}, \xi, \omega$ является соотношение, заявленное в условии теоремы. $\square$

Литература

1. K. Iwasawa, *On Galois groups of local fields.* — Trans. Amer. Soc. **80**, No. 2 (1955), 448–469.
2. K. Iwasawa, *On local cyclotomic fields.* — J. Math. Soc. Japan **12**, No. 1 (1960), 16–21.

3. M. Krasner, *Sur la représentation exponentielle dans les corps relativement galoisiens de nombres p-adiques.* — Acta arithm. **3** (1939), 133–173.
4. *Алгебраическая теория чисел*, под редакцией Дж. Касселса и А. Фрёлиха, М.: Мир, 1969.
5. З. И. Боревич, *Мультипликативная группа регулярного локального поля с циклической группой операторов.* — Изв. АН СССР, сер. матем. **24**, No. 2 (1960), 145–152.
6. З. И. Боревич, *О мультипликативной группе циклических p-расширений локального поля.* — Тр. МИАН СССР **80** (1965), 16–29.
7. З. И. Боревич, С. В. Востоков, *Кольцо целых элементов расширения простой степени локального поля как модуль Галуа.* — Зап. научн. семин. ЛОМИ **31** (1973), 24–37.
8. С. В. Востоков, *Идеалы абелева p – расширения локального поля как модули Галуа.* — Зап. научн. семин. ЛОМИ **57** (1976), 64–84.
9. В. А. Колывагин, *Формальные группы и символ норменного вычета.* — Изв. АН СССР, Сер. матем., **43**, No. 5 (1979), 1054–1120.

Vostokov S. V., Nekrasov I. I. Lubin–Tate formal module in a cyclic unramified p-extension as Galois module.

In this paper we describe the structure of the $\mathcal{O}_K[G]$-module $F(\mathfrak{m}_M)$, where M/L, L/K, $K/\mathbb{Q}_p$ are finite Galois extensions (p is fixed prime number), $G = \mathrm{Gal}(M/L)$, $\mathfrak{m}_M$ is a maximal ideal of M and F is a formal Lubin–Tate group law over $\mathcal{O}_K$ for a prime element π.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: sergei.vostokov@gmail.com

Поступило 23 сентября 2014 г.