Регулярные формальные модули в одномерных локальных полях *

С. М. Власьев, С. В. Востоков, А. А. Горшков

Аннотация

В работе исследуется проблема описания неразветвленных расширений локального поля, которые вместе с основным полем не содержат нетривиальных корней изогении формальной группы, заданной над кольцом целых этого поля. Эта задача возникла при изучении расширений без высшего ветвления для мультипликативных формальных групп в работе З. И. Боревича, 1962 г.

1 Введение

При исследовании нормальных расширений без высшего ветвления возникла задача описания всех неразветвленных расширений локального поля, которые вместе с основным полем являются регулярными, то есть не содержащими нетривиальных p-х корней из 1 (где p — характеристика поля вычетов локального поля). Основное локальное поле при этом называется вполне регулярным. Эта задача была решена З. И. Боревичем в работе [1]. Основной результат этой работы, доказательство которого было упрощено Д. К. Фаддеевым и приведено там же, является следующим.

 $Teopema~1.1.~(3.~M.~{\rm Боревич},~1962).~{\rm Для}~{\rm того},~{\rm чтобы}~{\rm локальное}~{\rm поле}~K~{\rm было}~{\rm вполне}~{\rm регулярным},~{\rm необходимо}~{\rm и}~{\rm достаточно},~{\rm чтобы}~{\rm показатель}~{\rm ветвления}~e~{\rm расширения}~K/{\mathbb Q}_p$ не делился на p-1.

Аналогичная задача возникает в арифметике формальных модулей. Она и решается в настоящей работе. Чтобы сформулировать эту задачу в общем случае, введем необходимые обозначения.

Пусть K — локальное поле, \mathfrak{O}_K — его кольцо целых, \mathfrak{M}_K — максимальный идеал в \mathfrak{O}_K , F(X,Y) — одномерная коммутативная формальная группа над \mathfrak{O}_K (далее мы будем писать просто формальная группа), i(X) — ее обратный элемент. Заметим, что на множестве \mathfrak{M}_K можно задать структуру группы:

$$(\alpha +_F \beta)(X) = F(\alpha, \beta), \ \alpha, \beta \in \mathfrak{M}_K$$

 $(-_F \alpha)(X) = i(\alpha), \ \alpha \in \mathfrak{M}_K.$

Теперь пусть π_0 — простой элемент в подполе K_0 поля K, F(X,Y) — формальная группа над \mathfrak{O}_K такая, что $\mathrm{End}_{\mathfrak{O}_K}(F) \cong \mathfrak{O}_{K_0}.$

^{*}Работа выполнена при поддержке гранта РФФИ № 14-01-00393.

Ключевые слова: локальное поле, вполне регулярное локальное поле, формальный модуль, формальная группа

Определение 1.1. Под формальным \mathfrak{O}_{K_0} -модулем $F(\mathfrak{M}_K)$ мы будем понимать \mathfrak{O}_{K_0} модуль, построенный на максимальном идеале \mathfrak{M}_K кольца целых \mathfrak{O}_K с помощью следующих операций:

$$\alpha +_F \beta := F(\alpha, \beta), \quad a \cdot \alpha := [a]_F(\alpha), \quad a \in \mathfrak{O}_{K_0}, \alpha, \beta \in \mathfrak{M}_K.$$

Определение 1.2. Обобщая определение регулярного локального поля в работе 3. И. Боревича, мы называем локальное поле K (а вместе с ним и формальный модуль $F(\mathfrak{M}_K)$) регулярным относительно формальной группы F, если K (а значит и $F(\mathfrak{M}_K)$) не содержит нетривиальных корней изогении $[\pi_0]_F$.

Onpedenehue 1.3. Будем называть локальное поле K (а вместе с ним и формальный модуль $F(\mathfrak{M}_K)$) вполне регулярным относительно формальной группы F, если любое его конечное неразветвленное расширение L/K (а значит и $F(\mathfrak{M}_L)$) является регулярным относительно формальной группы F.

Например, пусть $F_m = X + Y + XY$ — мультипликативная формальная группа. Эндоморфизмы умножения в F_m имеют вид: для $r \in \mathbb{N}$

$$[r]_{F_m}(x) = (1+x)^r - 1,$$

$$Ker[p]_{F_m} = \{\xi = (\zeta - 1)\},\$$

где ζ — первообразный корень p-ой степени из 1. Диаграмма полей выглядит в этом случае так:

$$\mathbb{Q}_p \longrightarrow L = K$$

$$\mathbb{Z}_p \longrightarrow \mathfrak{O}_K$$

$$p \longrightarrow \pi$$

$$p \longrightarrow \pi$$

Сформулируем теорему 1.1 в терминах регулярного формального модуля.

Теорема 1.2. Пусть K — регулярное локальное поле, $F_m(X,Y)$ — мультипликативная группа над \mathbb{Z}_p . Тогда поле K (а значит и формальный модуль $F_m(\mathfrak{M}_K)$) являются вполне регулярными относительно формальной группы F тогда и только тогда, когда индекс ветвления $e = e(K/\mathbb{Q}_p)$ не делится на p-1.

Таким образом, мы перенесли постановку задачи на область арифметики формальных модулей. Далее эта задача будет решаться для различных одномерных формальных групп (формальных модулей).

2 Основные обозначения

K — конечное алгебраическое расширение поля \mathbb{Q}_p ,

 K_0 — подполе в K,

T — подполе инерции в K со степенью инерции f_0 ,

 \mathfrak{O}_K — кольцо целых K, \mathfrak{O}_{K_0} — кольцо целых K_0 ,

 π — простой элемент \mathfrak{O}_K ,

 π_0 — простой элемент \mathfrak{O}_{K_0} ,

F(X,Y) — одномерная коммутативная формальная группа над \mathfrak{O}_K , причем $\operatorname{End}_{\mathfrak{O}_K}(F) \cong \mathfrak{O}_{K_0}$,

L — расширение поля K, не содержащее $\mathrm{Ker}_F[\pi_0]$ (без нуля),

 \mathfrak{O}_L — кольцо целых L,

 Π — простой элемент \mathfrak{O}_L .

Общая диаграмма (башня) полей выглядит так:

$$\mathbb{Q}_p \longrightarrow K_0 \longrightarrow K \longrightarrow L$$

$$\mathbb{Z}_p \longrightarrow \mathfrak{D}_{K_0} \longrightarrow \mathfrak{D}_K \longrightarrow \mathfrak{D}_L$$

$$p \longrightarrow \pi_0 \longrightarrow \pi \longrightarrow \Pi$$

3 Многочленная формальная группа

Пусть K — конечное расширение поля \mathbb{Q}_p и c — некоторая единица в K.

Определение 3.1. Формальную группу вида $F_c(X,Y) == X + Y + cXY$ назовем многочленной формальной группой.

Замечание 3.1. Известно, что $\operatorname{End}(F_c) \cong \mathbb{Z}_p$ (см. [2]), то есть в общем случае эта формальная группа не является группой Любина-Тейта. Однако, например, для $c \in \mathbb{Z}_p$ она таковой является.

Легко видеть, что

$$F_c(X,Y) = c^{-1}((1+cX)(1+cY)-1).$$

Тогда несложно доказать, что (см. например [3])

$$[p]_{F_c}(X) = c^{-1}([p]_{F_m}(cX)) = c^{-1}((1+cX)^p - 1),$$

 $\operatorname{Ker}[p]_{F_c} = \{\xi = c^{-1}(\zeta - 1)\},$

где ζ — первообразный корень p-ой степени из 1.

Пусть $\xi \in \text{Ker}[p]_{F_c}(X), \ \xi \neq 0.$

Лемма 3.1.

$$-p = ((\varepsilon(X)c)X)^{p-1}|_{X=\xi}, \text{ где } \varepsilon \in 1 + \mathbb{Z}_p[c][|X|]$$
 (1)

Доказательство. Действительно, из определения $[p]_{F_c}(X)$ получаем

$$\frac{[p]_{F_c}(X)}{X} = p + C_p^2 cX + \dots + C_p^{p-1} c^{p-2} X^{p-2} + (cX)^{p-1} = p\eta(X) + (cX)^{p-1},$$

где
$$\eta(X)=1+rac{C_p^2}{p}cX+\ldots+rac{C_p^{p-1}}{p}c^{p-2}X^{p-2}\in\mathbb{Z}[c][X].$$
 Поэтому

$$-p = \eta(X)^{-1} (cX)^{p-1}|_{X=\xi}$$

Так как $\eta(X)^{-1}\equiv 1 \mod(X)$, то найдется ряд $\varepsilon(X)\in \mathbb{Z}[c][|X|],\ \varepsilon(X)\equiv 1 \mod(X)$, такой что $\varepsilon(X)^{p-1}=\eta(X)^{-1}$. Тогда

$$-p = ((\varepsilon(X)c)X)^{p-1}|_{X=\mathcal{E}}$$

Пусть L — конечное расширение поля \mathbb{Q}_p и c — некоторая единица в L. Пусть $F_c(X,Y)$ — многочленная формальная группа над $\mathbb{Z}_p[c]$. Пусть $\xi \neq 0$ — корень изогении $[p]_{F_c}(X)$, причем $\xi \notin L$. Тогда диаграмма полей выглядит так:

$$\mathbb{Q}_p \longrightarrow \mathbb{Q}_p[c] \longrightarrow L$$

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p[c] \longrightarrow \mathfrak{I}_L$$

$$p \longrightarrow \pi \longrightarrow \Pi$$

Теорема 3.2. Поле L (а значит и $F_c(\mathfrak{M}_L)$) являются вполне регулярными относительно формальной группы $F_c(X,Y)$ тогда и только тогда, когда индекс ветвления $e=e(L/\mathbb{Q}_p)$ не делится на p-1.

Доказательство. Из равенства (1) леммы 3.1 следует, что

$$-p = (\varepsilon(\xi)c)^{p-1}\xi^{p-1},$$

то есть. $p-1/-p = (\varepsilon(\xi)c)\xi$. Отсюда получаем, что

$$L(\operatorname{Ker}[p]_{F_c}) = L(\xi) = L({}^{p-1}\sqrt{-p})$$
(2)

П

Пусть $-p = \Pi^e \theta u$, где Π — простой элемент в $L, \theta \in \Re$ — представитель Тейхмюллера в поле L, u — главная единица поля L.

1. Если $e \equiv 0 \mod (p-1)$, то

$$p-1\sqrt{-p} = \sqrt[p-1]{\prod^e \theta} u_1,$$

где $u_1^{p-1} = u, u_1 \in L$. Откуда

$$L(\sqrt[p-1]{-p}) = L(\sqrt[p-1]{\theta}),$$

то есть расширение $L(\sqrt[p-1]{-p})/L$ неразветвлено, а значит, согласно (2), расширение $L(\mathrm{Ker}[p]_{F_c})/L$ тоже неразветвлено, следовательно $F_c(\mathfrak{M}_L)$ не является вполне регулярным модулем.

2. Если $e \not\equiv 0 \mod (p-1)$, то

$$\sqrt[p-1]{-p} = \sqrt[p-1]{\prod^e \theta} u_1,$$

и $L(\sqrt[p-1]{-p})=L(\sqrt[p-1]{\Pi^e\theta})$ разветвлено над L, откуда $F_c(\mathfrak{M}_L)$ — вполне регулярный модуль.

3амечание 3.2. Условие неразветвленности получилось таким же, как и в случае мультипликативной формальной группы F_m .

4 Формальная группа Любина-Тейта

Определение 4.1. Пусть K — конечное расширение поля \mathbb{Q}_p . Введем \mathfrak{F}_{π} как множество формальных степенных рядов $f(X) \in \mathfrak{O}_K[|X|]$ таких, что

$$f(X) \equiv \pi X \mod deg \ 2, \ f(X) \equiv X^q \mod \pi,$$

где π — простой элемент в K и q — количество элементов поля частных поля K. Тогда по известной теореме (см. [4]) для каждого f(X) из \mathfrak{F}_{π} однозначно строится формальная группа F_{π} над \mathfrak{O}_K , которая называется формальной группой Любина-Тейта. При этом отображение $\mathfrak{O}_K \to \operatorname{End}_{\mathfrak{O}_K}(F_{\pi}): \alpha \mapsto [\alpha]_{F_{\pi}}$ является кольцевым гомоморфизмом и $f = [\pi]_{F_{\pi}}$.

Пусть формальная группа Любина-Тейта $F_{\pi}(X,Y)$ построена по изогении

$$[\pi](X) = \pi X + \pi a_2 X^2 + \ldots + X^q + \ldots$$
 (3)

Заметим, что в этом случае $\mathfrak{O}_{K_0} = \mathfrak{O}_K$, $K_0 = K$, $\pi_0 = \pi$. Пусть L — расширение поля K такое, что $\operatorname{Ker}_{F_{\pi}}[\pi]$ (без нуля) не содержится в L. Тогда диаграмма полей имеет вид:

$$\mathbb{Q}_p \longrightarrow K \longrightarrow L$$

$$\mathbb{Z}_p \longrightarrow \mathfrak{D}_K \longrightarrow \mathfrak{D}_L$$

$$p \longrightarrow \pi \longrightarrow \Pi$$

Теорема 4.1. Поле L (а значит и $F_{\pi}(\mathfrak{M}_{L})$) являются вполне регулярными относительно формальной группы F_{π} тогда и только тогда, когда индекс ветвления e = e(L/K) не делится на q-1.

Доказательство. Так как $F_{\pi}(X,Y)$ построена по изогении (3), то $[\pi](X)$ можно представить в виде:

$$[\pi](X) = \pi X \varepsilon(X) + X^q,$$

где $\varepsilon(X) \equiv 1 \mod X$. Заметим, что так как q-1 и p взаимно просты, то из ряда $\varepsilon(X)^{-1}$ в этом случае можно извлечь в кольце $\mathfrak{O}_K[|X|]$ корень степени q-1. То есть существует ряд $u(X) \in 1 + X\mathfrak{O}_K[|X|]$ такой, что $u(X)^{q-1} = \varepsilon(X)^{-1}$, поэтому

$$\frac{[\pi](X)}{X} = \pi u(X)^{-(q-1)} + X^{q-1}.$$

Получаем уравнение для корня изогении $X \neq 0$:

$$-\pi = (Xu(X))^{q-1} = Y^{q-1}.$$

Так как L — расширение поля K, Π — простой в L, то для e = e(L/K) :

$$-\pi = \Pi^e \theta \eta(\Pi),$$

где $\eta(\Pi) \equiv 1 \mod \Pi$ — главная единица.

1) Если e = (q - 1)e', то получим, что

$$-\pi = (\Pi^{e'}\eta_1(\Pi))^{q-1}\theta,$$

где
$$\eta_1^{q-1} = \eta$$
. И, значит,

$$Y = \Pi^{e'} \eta_1 \sqrt[q-1]{\theta},$$

где $\Pi^{e'}\eta_1 \in L$, а θ из неразветвленного расширения поля L. Таким образом, L(Y)/L — неразветвлено, а значит $F_{\pi}(\mathfrak{M}_L)$ не является вполне регулярным модулем.

2) Если e не делится на q-1, то $L(Y)=L(\sqrt[q-1]{-\pi})==L(\sqrt[q-1]{\Pi^e\theta})$ разветвлено над L, откуда $F_\pi(\mathfrak{M}_L)$ — вполне регулярный относительно группы F модуль.

5 Формальная группа Хонды

Пусть K — конечное неразветвленное расширение \mathbb{Q}_p . Рассмотрим \triangle — оператор Фробениуса в $\mathfrak{O}_K[|X|]$:

$$\triangle(\sum a_i x^i) = \sum a_i^{Fr} x^{p \cdot i}, \ a_i \in \mathfrak{O}_K,$$

где Fr — продолжение автоморфизма Фробениуса на K/\mathbb{Q}_p . Множество операторов $\sum_{i\geqslant 0}a_i\triangle^i$, где $a_i\in\mathfrak{O}_K$, образуют некоммутативное кольцо $\mathfrak{O}_K[|\, \triangle\, |]$ формальных степенных рядов от \triangle , для которого $\triangle a=a^{Fr}\triangle$ для $a\in\mathfrak{O}_K$.

Определение 5.1. Пусть K_0 — конечное расширение поля \mathbb{Q}_p, q — количество элементов поля частных поля K_0, K — конечное неразветвленное расширение K_0, π_0 — простой элемент в K_0 . Формальная группа F над \mathfrak{O}_K с логарифмом $\log_F(X) \in K[|X|]$ называется формальной групппой Хонды, если

$$u \circ \log_F \equiv 0 \mod \pi_0$$

для некоторого оператора $u = \pi_0 + a_1 \triangle + \ldots \in \mathfrak{O}_K[|\triangle|]$. Оператор u называется munom формальной группы F.

Пусть опять K_0 — конечное расширение поля \mathbb{Q}_p , K — конечное неразветвленное расширение K_0 . Рассмотрим F(X,Y) — группу Хонды над \mathfrak{O}_K высоты h такую, что $\mathfrak{O}_{K_0} \cong \operatorname{End}_{\mathfrak{O}_K} F$. Пусть L — расширение K такое, что $\operatorname{Ker}_F[\pi_0]$ (без нуля) не содержится в L. Тогда диаграмма полей имеет вид:

$$\mathbb{Q}_p \longrightarrow K_0 \longrightarrow K \longrightarrow L$$

$$\mathbb{Z}_p \longrightarrow \mathfrak{O}_{K_0} \longrightarrow \mathfrak{O}_K \longrightarrow \mathfrak{O}_L$$

$$p \longrightarrow \pi_0 \longrightarrow \pi_0 \longrightarrow \Pi$$

Теорема 5.1. Поле L (а значит и $F(\mathfrak{M}_L)$) являются вполне регулярными относительно формальной группы F тогда и только тогда, когда индекс ветвления e = e(L/K) не делится на $q^h - 1$.

Доказательство. Заметим, что $e=e(L/K)=e(L/K_0)$, так как расширение K/K_0 неразветвлено по условию.

Пусть π_0 — простой элемент в K_0 . Рассмотрим эндоморфизм формальной группы F умножения на π_0 :

$$[\pi_0]_F(X) = \pi_0 X + a_2 \pi_0 X^2 + \dots + a_{q^h} X^{q^h} + \dots, \quad a_i \in \mathfrak{O}_K$$

и $a_{q^h} \in \mathfrak{D}_K^*$, так как высота F равна h. Все коэффициенты $a_i \in \pi_0 \mathfrak{D}_K$, так как по условию расширение $\mathfrak{D}_K/\mathfrak{D}_{K_0}$ неразветвлено.

По подготовительной лемме Вейерштрасса существует $\varepsilon(X) \in 1 + X\mathfrak{O}_{K_0}[|X|]$ такой, что

$$f(X) := \frac{[\pi_0](X)}{X} \varepsilon(X) = \pi_0 + \pi_0 c_1 X^1 + \ldots + \pi_0 c_{q^h - 2} X^{q^h - 2} + c_{q^h - 1} X^{q^h - 1},$$

где $c_{q^h-1} \in \mathfrak{O}_K^*$.

Ясно, что

$$\operatorname{Ker}[\pi_0]_F(X) = \operatorname{Ker} f(X)$$

Пусть π — корень многочлена f(X) и соответственно, ненулевой корень $[\pi_0](X)=0$, тогда расширение $K(\pi)/K$ вполне разветвлено и π — простой элемент в нем. Поэтому в поле $K(\pi)$ имеем:

$$-\pi_0(1+c_1\pi+\ldots+c_{q^h-2}\pi^{q^h-2})=c_{q^h-1}\pi^{q^h-1},$$

откуда

$$-\pi_0 = c_{q^h - 1} \pi^{q^h - 1} \varepsilon,$$

где $\varepsilon = (1 + c_1 \pi + \ldots + c_{q^h - 2} \pi^{q^h - 2})^{-1}.$

Пусть ε' — единица в $K(\pi)$ такая, что $(\varepsilon')^{q^h-1}=\varepsilon$, тогда $\pi'=\pi\varepsilon'$ будет корнем уравнения

$$X^{q^h-1} + \pi_0' = 0,$$

где $\pi_0' = \pi_0 c_{a^h-1}^{-1} \in K_0$. При этом

$$L(\operatorname{Ker}[\pi_0]_F) = L(\pi) = L(\pi'),$$

так как $\mathrm{Ker}[\pi_0]_F$ не принадлежит по условию полю L. Но $K\subset L$, а уравнение

$$c_{q^h-1}X^{q^h-1} + \pi_0(1 + c_1X + \dots + c_{q^h-2}X^{q^h-2}) = 0$$

равносильно уравнению

$$Y^{q^h-1} + \pi_0 c_{q^h-1}^{-1} = 0 \Leftrightarrow Y^{q^h-1} + \pi'_0 = 0,$$

где

$$Y = X(1 + c_1X + \ldots + c_{q^h-2}X^{q^h-2})^{-1}.$$

Итак, мы доказали, что

$$L(\operatorname{Ker}[\pi_0]_F) = L(\pi'),$$

где π' — корень уравнения $X^{q^h-1} + \pi'_0 = 0, \pi'_0$ — простой в K_0 (и в K).

1. Пусть индекс ветвления e=e(L/K) делится на q^h-1 , то есть $e=(q^h-1)e'$, и пусть Π — простой элемент в L. Тогда

$$-\pi_0' = \Pi^e \theta \eta$$
,

где θ — представитель Тейхмюллера, а η — главная единица поля L. Тогда

$$\pi' = \sqrt[q^h - 1]{-\pi'_0} = \Pi^{e'} \sqrt[q^h - 1]{\theta} \eta_1,$$

где
$$\eta_1^{q^h-1}=\eta$$
 в $L.$

Поэтому расширение $L(\pi') = L({}^{q^h} \sqrt[1]{\theta})$, а с ним и $L(\text{Ker}[\pi_0]_F)$ неразветвлено над L. Это значит, что $F(\mathfrak{M}_L)$ не является вполне регулярным модулем.

2. Если же e не делится на $q^h - 1$, то расширение $L(\pi') = L(\sqrt[q^h - 1]{\pi^e \theta})$ будет разветвлено над L, откуда $F(\mathfrak{M}_L)$ — вполне регулярный относительно группы F модуль.

Заключение

Фактически, исследование регулярных формальных модулей до этого было выполнено только для случая мультипликативной формальной группы одномерного локального поля в работе З. И. Боревича [1]. В данной работе сделан следующий шаг к обобщению результатов — получены свойства для случая многочленной формальной группы, для формальной группы Любина-Тейта и формальной группы Хонды.

Остается открытым вопрос о произвольных формальных модулях как в одномерных, так и в многомерных локальных полях. Кроме того, возникает вопрос об условиях для неразветвленного кругового поля, содержащего все корни p-ой степени из 1. Эти вопросы мы постараемся исследовать в следующих работах.

Список литературы

- [1] З. И. Боревич, О регулярных локальных полях, Вестник ЛГУ, 1962, стр. 142-145.
- [2] M. Hazewinkel, Formal groups and applications, Academic Press, New York, 1978.
- [3] С. В. Востоков, П. П. Волков, Г. К. Пак, Символ Гильберта для многочленных формальных групп, Зап. науч. сем. ПОМИ, том 400, 2012, стр. 127-132.
- [4] I. B. Fesenko, S. V. Vostokov, Local Fields and Their Extensions, Second edition, 2002.
- [5] Д. Г. Бенуа, С. В. Востоков, Арифметика группы точек формальной группы, Зап. научн. сем. ЛОМИ, 191 (1991), стр. 9–23.
- [6] I. B. Zhukov, Higher dimensional local fields, Invitation to higher local fields, 2000, crp. 5-18.
- [7] T. Honda, On the theory of commutative formal groups, J. Math Soc. Japan, 1970, crp. 213-246.
- С. М. Власьев, аспирант Математико-Механического факультета СПБГУ, 198504, Россия, Санкт-Петербург, Старый Петергоф, Университетский проспект, дом 28

E-mail: svlassiev@gmail.com Tелефон: +79117448297

С. В. Востоков, д.Ф.-м.н., профессор СПБГУ, Математико-Механический факультет, 198504, Россия, Санкт-Петербург, Старый Петергоф, Университетский проспект, дом 28

E-mail: sergei.vostokov@gmail.com Телефон: +78129584600

А. А. Горшков, аспирант Математико-Механического факультета СПБГУ, 198504, Россия, Санкт-Петербург, Старый Петергоф, Университетский проспект, дом 28