УДК 512.741 Вестник СПбГУ. Математика. Механика. Астрономия. 2020. Т. 7 (65). Вып. 4
MSC 11S31

Степень иррегулярности и регулярные формальные модули в локальных полях*

Н. К. Власкина[1], *С. В. Востоков*[1], *П. Н. Питаль*[1], *А. Е. Цыбышев*[2]

[1] Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9
[2] Санкт-Петербургское отделение математического института им. В. А. Стеклова РАН,
Российская Федерация, 191023, Санкт-Петербург, наб. р. Фонтанки, 27

Для цитирования: *Власкина Н. К., Востоков С. В., Питаль П. Н., Цыбышев А. Е.* Степень иррегулярности и регулярные формальные модули в локальных полях // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. 2020. Т. 7 (65). Вып. 4. С. 588–596. https://doi.org/10.21638/spbu01.2020.402

В работе исследуется изменение степени иррегулярности при конечных неразветвленных расширениях локального поля относительно многочленной формальной группы и в мультипликативном случае. Для всех целых положительных чисел s получены необходимые и достаточные условия на наличие первообразных корней p^s-й степени из 1 (эндоморфизма $[p^s]_{F_m}$) в L-конечном неразветвленном расширении локального поля K. Эти условия зависят лишь от индекса ветвления максимального абелева подрасширения поля K $K_a/\mathbb{Q}_p$.

Ключевые слова: регулярные формальные модули, формальные модули, формальные группы, локальные поля.

1. Введение. В теории локальных полей при изучении строения группы Галуа замыкания локального поля возникает вопрос о том, при каких условиях присоединение к регулярному локальному полю корня степени p из 1 дает неразветвленное расширение. Теорема, доказанная З. И. Боревичем в работе [1], доказательство которой впоследствие упростил Д. К. Фаддеев, сформулирована ниже (утверждение 1.3).

Определение 1.1. Локальное поле называется *регулярным*, если оно не содержит первообразных корней степени p из 1.

Определение 1.2. *Степенью иррегулярности локального поля K* называется такое целое положительное число s, что данное поле содержит первообразный корень степени p^s, но не содержит первообразный корень степени p^{s+1}.

Легко видеть, что, если разрешить s равняться 0, то регулярное поле — это поле степени иррегулярности $s = 0$.

Утверждение 1.3. *Пусть K — регулярное локальное поле. Расширение $K(\zeta)/K$, где $\zeta^p = 1$, $\zeta \neq 1$, будет неразветвленным тогда и только тогда, когда индекс ветвления $e = e(K_a/\mathbb{Q}_p)$ делится на $p-1$. $K_a/\mathbb{Q}_p$ — максимальное абелево подрасширение в $K/\mathbb{Q}_p$.*

*Работа выполнена при поддержке Российского научного фонда (грант № 16-11-10200).

Кроме того, в работе [2] доказано аналогичное утверждение для формальных модулей.

Пусть K — локальное поле, F — одномерная коммутативная формальная группа над кольцом целых $\mathcal{O}_K$ (дальше мы будем писать просто формальная группа). Пусть π_0 — простой элемент в подполе K_0 поля K.

Определение 1.4. Под *формальным модулем* $F(\mathfrak{M}_K)$ будем понимать $\mathcal{O}_{K_0}$-модуль, построенный на максимальном идеале $\mathfrak{M}_K$ кольца целых при помощи операций $a +_F b = F(a, b)$ и $\alpha \cdot a = [\alpha]_F(a), a, b \in \mathfrak{M}_K, \alpha \in \mathcal{O}_{K_0}$.

Определение 1.5. Локальное поле K (а вместе с ним и формальный $\mathcal{O}_{K_0}$-модуль $F(\mathfrak{M}_K)$) называется *регулярным относительно формальной группы* F, если K (а значит, и $F(\mathfrak{M}_K)$) не содержит нетривиальных корней изогении $[\pi_0]_F$.

Определение 1.6. Локальное поле K (а вместе с ним и формальный $\mathcal{O}_{K_0}$-модуль $F(\mathfrak{M}_K)$) называется *вполне регулярным относительно формальной группы* F, если всякое конечное неразветвленное расширение L/K (и формальный модуль $F(\mathfrak{M}_L)$) регулярно относительно F.

В следующем определении мы будем предполагать, что K_0 не разветвлено над $\mathbb{Q}_p$. Поэтому в этом случае в качестве π_0 можно взять p.

Определение 1.7. Будем называть *степенью иррегулярности формального модуля* $F(\mathfrak{M}_K)$ такое число $s \geqslant 0$, что K (а значит, и $F(\mathfrak{M}_K)$) не содержит элементов из $\{Ker[p^{s+1}] \setminus Ker[p^s]\}$, но содержит нетривиальные корни ядра $Ker[p^s]$.

Утверждение 1.8. *Поле L, а значит, и $F_c(\mathfrak{M}_L)$, являются вполне регулярными относительно многочленной формальной группы $F_c(X, Y)$ тогда и только тогда, когда индекс ветвления $e = e(L/\mathbb{Q}_p)$ не делится на $p - 1$.*

Утверждения 1.3 и 1.8 дают ответ, увеличилась ли степень иррегулярности у расширения регулярного локального поля (то есть поля степени иррегулярности $s = 0$), зависящая лишь от индекса ветвления.

В настоящей работе сделана попытка обобщить данную конструкцию для всех целых неотрицательных s, а именно доказаны следующие утверждения.

Теорема 1.9. *Всякое конечное неразветвленное расширение L/k локального поля k не содержит первообразного корня степени p^{s+1} из 1, $\zeta_{p^{s+1}}$, в том и только в том случае, когда $(p-1)p^s \not| \, e_0$.*

Этот результат также обобщен на случай формальных модулей, соответствующих многочленной формальной группе $x + y + cxy$ над $\mathcal{O}_K, c \in \mathcal{O}_K^*$.

Теорема 1.10. *Пусть k — локальное поле, F — многочленная формальная группа $x + y + cxy, c \in \mathcal{O}_k^*$. Тогда для любого неразветвленного L/k ядро эндоморфизма $[p^{s+1}]_F$ на m_L совпадает с ядром эндоморфизма $[p^s]_F$ в том и только в том случае, когда индекс ветвления максимального абелева подрасширения $k_a/\mathbb{Q}_p$ не делится на $(p-1)p^s$.*

2. Необходимые определения из теории формальных групп.

Определение 2.1. Пусть A — коммутативное ассоциативное кольцо с 1. Формальный степенной ряд $F(X, Y) \in A[[X, Y]]$ такой, что:

1) $F(X,0) = X, F(0,Y) = Y$,

2) $F(X,F(Y,Z)) = F(F(X,Y),Z)$,

будем называть (*одномерным*) *формальным групповым законом над* A, а пару F/A — (*одномерной*) *формальной группой.* Если также верно, что

3) $F(X,Y) = F(Y,X)$,

то такой формальный групповой закон называется *коммутативным.*

Определение 2.2. Пусть F, G — (одномерные) формальные групповые законы над кольцом A. *Гомоморфизмом* из F в G называется формальный степенной ряд $f(X) \in A[[X]]$ такой, что $G(f(X), f(Y)) = f(F(X,Y))$.

Определение 2.3. Гомоморфизмы из F в F называются *эндоморфизмами* F. В случае, если F коммутативен, они образуют кольцо с операцией сложения $f+g = F(f,g)$ и композицией в качестве умножения.

Определение 2.4. Пусть L — локальное поле, $A = \mathcal{O}_L$ — его кольцо целых, $\mathfrak{M}_L$ — его максиальный идеал, F — коммутативный (одномерный) формальный групповой закон над A, и $B = End(F)$. *Формальным B-модулем* $F(\mathfrak{M}_L)$ будем называть B-модуль на $\mathfrak{M}_L$ с операциями $a +_F b = F(a,b)$ и $\alpha \cdot a = [\alpha]_F(a)$, $\alpha \in B, a, b \in \mathfrak{M}_L$.

Если $n \in \mathbb{N}$, то $[n]_F(a) = a +_F a + \cdots +_F a$ (n слагаемых). В простейших случаях для этого эндоморфизма можно написать явную формулу.

Пример 2.5. Если $F = F_a$ — аддитивная формальная группа $x+y$, то $[n]_{F_a}(b) = b + b + \cdots + b = n \cdot b$.

Пример 2.6. Если $F = F_m$ — мультипликативная формальная группа $x+y+xy$, то $[n]_{F_m}(b) = (\cdots((1+b)(1+b)-1)+1)(1+b)\cdots(1+b)-1) = (1+b)^n - 1$.

Пример 2.7. Если F — многочленная формальная группа $x + y + cxy$, то $[n]_F(b) = (\cdots c^{-1}((1+cb)(1+cb)-1)+1)(1+cb)\cdots(1+cb)-1) = (c^{-1}(1+cb)^n - 1)$.

3. Два утверждения о корнях изогений формальных модулей. Пусть L — локальное поле, c — единица в L, F — многочленный формальный групповой закон $X + Y + cXY$ над L. Переформулируем утверждение 1.8.

Утверждение 3.1. *Для любого конечного неразветвленного расширения полей L'/L изогения $[p]_F$ на $\mathfrak{M}_{L'}$ не имеет нетривиальных корней в том и только в том случае, когда индекс ветвления $e = e(L/\mathbb{Q}_p)$ не делится на $p-1$.*

Доказательство данного утверждения можно найти в [2, теорема 3.2]. Можно сформулировать обобщение на случай изогении $[p^{s+1}]_F$.

Теорема 3.2. *Для любого поля L' — конечного неразветвленного расширения поля L — $Ker[p^{s+1}]_F = Ker[p^s]_F$ на $\mathfrak{M}_{L'}$ тогда и только тогда, когда $e = e(L/\mathbb{Q}_p)$ не делится на $p^s(p-1)$.*

Замечание 3.3. $p-1 = \varphi(p) = |Gal(\mathbb{Q}_p[\zeta_p]/\mathbb{Q}_p)|$, где ζ_p — первообразный корень степени p из 1. В то же время $(p-1)p^s = \varphi(p^{s+1}) = |Gal(\mathbb{Q}_p\zeta_{p^{s+1}}]/\mathbb{Q}_p)|$.

На первый взгляд кажется разумным попробовать обобщить доказательство предыдущего утверждения на случай изогении $[p^{s+1}]_F$, но в ходе доказательства извлекается корень степени $p-1$ из ряда, что в случае обобщения превратилось бы в извлечение корня степени $p^s(p-1)$. При $s>0$ такой корень может не извлечься. Поэтому проведем доказательство, использующее локальную теорию полей классов.

4. Основные обозначения и вспомогательные утверждения. В данной работе k — локальное поле, то есть конечное расширение поля $\mathbb{Q}_p$. Вспомним некоторые определения. Пусть L/k — конечное расширение полей, $\alpha \in L$. L обладает операциями сложения и умножения на элементы из k и является над ним конечномерным векторным пространством. Оператор $m_\alpha : \beta \mapsto \alpha\beta$ является k-линейным оператором на L, поэтому у него есть определитель $\det(m_\alpha)$.

Определение 4.1. Пусть L/k — конечное расширение полей. *Отображением нормы* $N_{L/k} : L \to k$ называется следущее отображение: $N_{L/k}(\alpha) = \det(m_\alpha)$.

Определение 4.2. Пусть K — поле. *Дискретным нормированием на* K называется отображение $\nu : K \to \mathbb{Z} \cup \{+\infty\}$, обладающее следующими свойствами:

- $\nu(0) = \infty$,
- $\nu(a \cdot b) = \nu(a) + \nu(b)$,
- $\nu(a+b) \geq \min(\nu(a), \nu(b))$.

На поле K задано нормирование. Тогда можно естественным образом определить над K структуру нормированного поля, взяв в качестве нормы $||x|| := \nu(x)$ для $b>0$ и $b<1$. Будем предполагать, что все встречающиеся далее поля полны относительно норм.

Определение 4.3. *Кольцом целых поля* K называется его следующее подкольцо: $\mathcal{O}_k = \{x \in K : \nu(x) \geq 0\}$.

В кольце $\mathcal{O}_k$ имеется простой элемент π_k, единственный с точностью до умножения на обратимый, и $\nu_k(\pi_k) = 1$.

Определение 4.4. *Группой единиц локального поля* k называется группа $\mathcal{O}_k^*$.

Пусть L/k — конечное расширение локальных полей.

Определение 4.5. *Индексом ветвления* L *над* k называется число $e = \nu_L(\pi_k)$.

Определение 4.6. *Степенью инерции* L *над* k называется степень расширения конечных полей $(\mathcal{O}_L/\mathfrak{M}_L)/(\mathcal{O}_k/\mathfrak{M}_k)$.

Пусть k_a — максимальное абелево подрасширение в $k/\mathbb{Q}_p$, f_0, e_0 — степень инерции и индекс ветвления $k_a/\mathbb{Q}_p$ соответственно, $E = \mathbb{Z}_p^*$, $E_1 \subseteq E$ — подгруппа тех единиц, которые сравнимы с 1 по модулю p. Если L — локальное поле, то $\mathcal{O}_L$ обозначает его кольцо целых. Нам понадобятся следующие факты из локальной теории полей классов.

Факт 4.7 (см. [3, предложение VI.2.3 и теорема VI.2.2])**.** *Пусть K — локальное поле. Тогда существует обращающее включение взаимно однозначное соответствие между всеми конечными абелевыми расширениями K и некоторыми подгруппами в K^*, при этом расширению L/K сопоставляется его группа норм $N_{L/K}(L^*)$. Кроме того, есть канонический изоморфизм $Gal(L/K) \simeq K^*/N_{L/K}(L^*)$.*

Факт 4.8. *Пусть L_a/K — абелево расширение локальных полей степени инерции f и индекса ветвления e. Тогда группа норм $N_{L_a/K}(L_a^*) = \{\pi^f \cdot \varepsilon\} \times E'$, где π — простой элемент K, $\varepsilon \in \mathcal{O}_K^*$, а E' — подгруппа в $\mathcal{O}_K^*$ индекса e.*

Поскольку автор не нашел формулировку данного факта в литературе, ниже приводится его доказательство.

Доказательство. $L_a^* = \{\pi_{L_a}\} \times \mathcal{O}_{L_a}^*$, где π_{L_a} — простой элемент L_a. Поскольку норма единицы является единицей, а норма простого элемента нет, отображение нормы переводит это прямое произведение в прямое произведение, то есть $N_{L_a/K}(L_a^*) = \{N_{L_a/K}(\pi_{L_a})\} \times N_{L_a/K}(\mathcal{O}_{L_a}^*)$. Но $N_{L_a/K}(\pi_{L_a})$ имеет L_a-нормирование, равное $[L:k]$, поскольку норма $N_{L_a/K}(\pi_{L_a})$ равна произведению всех сопряженных $\prod\limits_{\sigma \in Gal(L_a/K)} \sigma(\pi_{L_a})$, а также поскольку действие групы Галуа сохраняет нормирование.

При этом L_a-нормирование в ограничении на K отличается от K-нормирования умножением на e по определению индекса ветвления. Значит, K-нормирование $N_{L_a/K}(\pi_{L_a})$ равно $[L_a : K]/e = f$ по [3, предложение I.5.3]. Каждый элемент такого нормирования представляется как $\pi^f \cdot \varepsilon$, $\varepsilon \in \mathcal{O}_K^*$. Обозначим за E' группу $N_{L_a/K}(\mathcal{O}_{L_a}^*)$. По факту 4.7 имеем $Gal(L_a/K) \simeq K^*/N_{L_a/K}(L_a^*) \simeq (\{\pi\} \times \mathcal{O}_K^*) \,/\, (\{\pi^f \cdot \varepsilon\} \times E')$. В последнем факторе можно построить фильтрацию с двумя подфакторами $\{\pi\} \times \mathcal{O}_K^*/\{\pi^f \cdot \varepsilon\} \times \mathcal{O}_K^*$ и $\{\pi^f \cdot \varepsilon\} \times \mathcal{O}_K^*/\{\pi^f \cdot \varepsilon\} \times E'$. Второй из них изоморфен $\mathcal{O}_K^* \times E'$. Первый же равен $\{\pi\} \times \mathcal{O}_K^*/\{\pi^f\} \times \mathcal{O}_K^*$, а потому изоморфен $\{\pi\}/\{\pi^f\}$ и равен циклической группе $\mathbb{Z}/f\mathbb{Z}$. В частности, он имеет порядок f. Так как по [3, предложение I.5.3] имеем $e \cdot f = |Gal(L_a/K)|$, порядок второго члена фильтрации равен $|Gal(L_a/K)|/f = e$, то есть E' — подгруппа индекса e, что завершает доказательство данного факта. $\square$

Факт 4.9. *Пусть K — локальное поле, L/K — конечное расширение, L_a — максимальное абелево подрасширение в L/K. Тогда группы норм L и L_a над K совпадают: $N_{L/K}(L^*) = N_{L_a/K}(L_a^*)$.*

Также понадобятся следующие леммы из статьи [1] с небольшой модификацией.

Лемма 4.10 (ср. [1, лемма 1]). *Пусть k_a — абелево расширение $\mathbb{Q}_p$ степени инерции f_0 и показателя разветвления e_0. Пусть $(p-1)p^s | e_0 (s \geqslant 0)$. Тогда группа норм $k_a/\mathbb{Q}_p$ содержится в группе вида $\{p^{f_0} \cdot \varepsilon\} \times E_1^{p^s}, \varepsilon \in \mathbb{Z}_p^*$.*

Доказательство. Поскольку группа $Gal(k_a/\mathbb{Q}_p)$ абелева, легко построить подрасширение k_a' со степенью инерции f_0 и индексом ветвления $(p-1)p^s$. По [1, лемма 1] имеем $N_{k_a'/\mathbb{Q}_p}((k_a')^*) = \{p^{f_0} \cdot \varepsilon\} \times E_1^{p^s}, \varepsilon \in \mathbb{Z}_p^*$. Но по факту 4.7 получаем $N_{k_a/\mathbb{Q}_p}(k_a^*) \subseteq N_{k_a'/\mathbb{Q}_p}((k_a')^*)$. $\square$

Лемма 4.11 [1, лемма 2]. *Пусть ζ_p^{s+1} — первообразный корень степени p^{s+1} из 1. Группа $\{p\} \times E_1^{p^s}$ является группой норм для расширения $\mathbb{Q}_p[\zeta_{p^{s+1}}]/\mathbb{Q}_p$.*

Также докажем вспомогательную лемму.

Лемма 4.12. *Пусть L — конечное неразветвленное расширение k. Тогда группы норм их единиц в $\mathbb{Q}_p$ совпадают: $N_{L/\mathbb{Q}_p}(L^*) = N_{k/\mathbb{Q}_p}(k^*) = E_0$.*

Доказательство. Поскольку L/k неразветвлено, то и максимальное абелево подрасширение L_ak/k неразветвлено.

По факту 4.9 имеем $N_{L/k}(L^*) = N_{L_ak/k}(L^*_{ak})$. Отсюда следует, что $N_{L/k}(\mathcal{O}^*_L) = N_{L_ak/k}(\mathcal{O}^*_{L_ak})$. При этом последняя группа по факту 4.8 равна $\mathcal{O}^*_k$. Но тогда $N_{L/\mathbb{Q}_p}(\mathcal{O}^*_L) = N_{k/\mathbb{Q}_p}(N_{L/k}(\mathcal{O}^*_L)) = N_{k/\mathbb{Q}_p}(\mathcal{O}^*_k) = E_0$. □

5. Сведение общего случая к мультипликативному. В этом разделе мы продемонстрируем, как можно свести задачу о корнях эндоморфизма в формальном модуле к мультипликативному случаю.

Доказательство. Легко видеть, что $F(X,Y) = c^{-1}((1+cX)(1+cY)-1)$. Тогда $[p]_F(X) = c^{-1}([p]_{F_m}(cX)) = c^{-1}((1+cX)^p - 1)$, где $F_m(X,Y) = X + Y + XY$ — мультипликативный формальный групповой закон. $Ker[p^{s+1}]_F = c^{-1}Ker[p^{s+1}]_{F_m}$. Аналогично для случая p^s. Таким образом, достаточно решить задачу для мультипликативного формального группового закона. □

Предложение 5.1. *Пусть k — локальное поле, F_m — мультипликативная формальная группа $x+y+xy$. Тогда для любого конечного неразветвленного расширения L/k ядро эндоморфизма $[p^{s+1}]_{F_m}$ совпадает с ядром $[p^s]_{F_m}$ в том и только в том случае, когда индекс ветвления максимального абелева подрасширения $k_a/\mathbb{Q}_p$ не делится на $(p-1)p^s$.*

Доказательство. $[p^{s+1}]_{F_m} = (1+X)^{p^{s+1}} - 1$ $Ker[p^{s+1}] = \{\xi \in \mathfrak{M}_L : (1+\xi)^{p^{s+1}} = 1\}$, то есть $1 + Ker[p^{s+1}]$ — множество всех корней степени p^{s+1} из 1 в множестве $1 + \mathfrak{M}_L$. Но поскольку поле вычетов $\mathcal{O}_L/\mathfrak{M}_L$ имеет характеристику p, в нем единственный корень из 1 степени p^{s+1} — это 1. Значит, все корни степени p^{s+1} из 1 в L лежат в $1 + \mathfrak{M}_L$, а значит $Ker[p^{s+1}] = \{\xi = \zeta - 1\}$, где ζ — корень p^{s+1} степени из 1. Аналогично для степени p^s.

Тем самым ядра совпадают тогда и только тогда, когда множества корней из 1 совпадают, то есть в поле L нет первообразного корня степени p^{s+1}. □

Пусть k — локальное поле, то есть конечное расширение поля $\mathbb{Q}_p$. Обозначим f_0, e_0 — степень инерции и индекс ветвления максимального абелева подрасширения $k_a/\mathbb{Q}_p$ соответственно. Пусть $E_0 \subset \mathbb{Q}^*_p$ — группа норм единиц из k. Пусть E — группа всех единиц в $\mathbb{Z}_p$, а $E_1 \subseteq E$ — подгруппа единиц, сравнимых с 1 по модулю p.

Предложение 5.2. *Всякое конечное неразветвленное расширение L/k не содержит первообразного корня степени p^{s+1} из 1, $\zeta_{p^{s+1}}$, в том и только в том случае, когда $(p-1)p^s \nmid e_0$.*

Таким образом, мы свели задачу к мультипликативному случаю. Поэтому для доказательства основного результата достаточно доказать предложение 5.2. Этому будет посвящен следующий раздел.

6. Мультипликативный случай. Для доказательства эквивалентности условий предложения 5.2 переформулируем оба условия на языке групп норм, докажем их эквивалентность.

Лемма 6.1. *Пусть L — конечное расширение $\mathbb{Q}_p$, тогда $\zeta_{p^{s+1}} \in L \Leftrightarrow N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$.*

Доказательство. Заметим, что первообразный корень степени p^{s+1} лежит в L тогда и только тогда, когда $L \supseteq \mathbb{Q}_p[\zeta_{p^{s+1}}]$. Далее заметим, что $\mathbb{Q}_p[\zeta_{p^{s+1}}]/\mathbb{Q}_p$ — абелево расширение, $L \supseteq \mathbb{Q}_p[\zeta_{p^{s+1}}] \Leftrightarrow L_a \supseteq \mathbb{Q}_p[\zeta_{p^{s+1}}]$, где L_a — максимальное абелево подрасширение в $L/\mathbb{Q}_p$. По факту 4.7 имеем $L_a \supseteq \mathbb{Q}_p[\zeta_{p^{s+1}}] \Leftrightarrow N_{L_a/\mathbb{Q}_p}(L_a^*) \subseteq N_{\mathbb{Q}_p[\zeta_{p^{s+1}}]/\mathbb{Q}_p}\left(\mathbb{Q}_p[\zeta_{p^{s+1}}]^*\right)$. По факту 4.9 $N_{L/\mathbb{Q}_p}(L^*) = N_{L_a/\mathbb{Q}_p}(L_a^*)$. По лемме 4.11 получаем $N_{\mathbb{Q}_p[\zeta_{p^{s+1}}]/\mathbb{Q}_p}\left(\mathbb{Q}_p[\zeta_{p^{s+1}}]^*\right) = \{p\} \times E_1^{p^s}$. Значит, $N_{L_a/\mathbb{Q}_p}(L_a^*) \subseteq N_{\mathbb{Q}_p[\zeta_{p^{s+1}}]/\mathbb{Q}_p}\left(\mathbb{Q}_p[\zeta_{p^{s+1}}]^*\right) \Leftrightarrow N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$. Тем самым, $\zeta_{p^{s+1}} \in L \Leftrightarrow N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$. □

Лемма 6.2. *Для того чтобы E_0 содержалось в $E_1^{p^s}$, необходимо и достаточно, чтобы индекс ветвления максимального абелева подрасширения $k_a/\mathbb{Q}_p$ делился на $(p-1)p^s$.*

Доказательство. Достаточность непосредственно следует из леммы 4.10. Для доказательства необходимости достаточно заметить, что в таком случае $e_0 = (E_0 : E) \vdots (E_1^{p^s} : E) = (p-1)p^s$ по теореме Лагранжа. □

Предложение 3.2 переформулируется на языке групп норм следующим образом.

Предложение 6.3. *Существует поле L — конечное неразветвленное расширение поля K такое, что $N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s} \Leftrightarrow E_0 \subseteq E_1^{p^s}$.*

Доказательство. Пусть L/k такое, что $N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$. Тогда по лемме 4.12 получаем $E_0 \subseteq N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$, следовательно, $E_0 \subseteq E_1^{p^s}$.

Пусть теперь $E_0 \subseteq E_1^{p^s}$, а L — произвольное неразветвленное расширение k степени $(p-1)p^s$. Группа норм $N_L/\mathbb{Q}_p(L^*)$ поля L равна $\{N_{L/\mathbb{Q}_p}(\pi)\} \times E_0$, где π — произвольный простой элемент поля L. Действительно, $L^* = \{\pi\} \times \mathcal{O}_L^*$, и отображение нормы переводит это разложение в разложение $\{N_{L/\mathbb{Q}_p}(\pi)\} \times N_{L/\mathbb{Q}_p}(L^*) = \{N_{L/\mathbb{Q}_p}(\pi)\} \times E_0$. Поскольку L/k неразветвлено, возьмем в качестве π простой элемент k. Поскольку норма элемента из базового поля вычисляется определителем диагональной матрицы, а потому равна этому элементу, возведенному в степень, равную степени расширения, $N_{L/k}(\pi) = \pi)^{(p-1)p^s}$. Поскольку норма функториальна, $N_{L/\mathbb{Q}_p}(\pi) = N_{k/\mathbb{Q}_p}(N_{L/k}(\pi)) = N_{k/\mathbb{Q}_p}(\pi^{(p-1)p^s})$, а поскольку отображение нормы мультипликативно, $N_{k/\mathbb{Q}_p}(\pi^{(p-1)p^s}) = N_{k/\mathbb{Q}_p}(\pi)^{(p-1)p^s}$. Тем самым, $N_{L/\mathbb{Q}_p}(\pi) = N_{k/\mathbb{Q}_p}(\pi)^{(p-1)p^s}$.

Раскладывая $N_{k/\mathbb{Q}_p}(\pi)$ как $p^f \cdot \varepsilon$ (f — степень инерции $k/\mathbb{Q}_p$), получаем $N_{L/\mathbb{Q}_p}(\pi) = p^{(p-1)p^s f} \cdot \varepsilon^{(p-1)p^s}$. При этом $\varepsilon^{(p-1)p^s} = (\varepsilon^{p-1})^{p^s} \in E_1^{p^s}$. Поэтому

$$\{N_{L/\mathbb{Q}_p}(\pi)\} \times E_0 = \{p^{(p-1)p^s f} \cdot \varepsilon^{(p-1)p^s}\} \times E_0 \subseteq \{p^{(p-1)p^s f} \cdot \varepsilon^{(p-1)p^s}\} \times E_1^{p^s}.$$

Но в абелевых группах, если элемент $g \in G$ не имеет кручения, $G = \{g\} \times H$, $h \in H$, то $G = \{gh\} \times H$. В нашем случае, поскольку $\varepsilon^{(p-1)p^s} \in E_1^{p^s}$,

$$\{p^{(p-1)p^s f} \cdot \varepsilon^{(p-1)p^s}\} \times E_1^{p^s} = \{p^{(p-1)p^s f}\} \times E_1^{p^s} \subseteq \{p\} \times E_1^{p^s}.$$

Итак, получаем $N_L/\mathbb{Q}_p(L^*) \subseteq \{p\} \times E_1^{p^s}$. □

Теперь совсем несложно доказать предложение 3.2.

Доказательство. По лемме 6.1 $\exists L/k$ конечное неразветвленное : $\zeta_{p^{s+1}} \in L$, если и только если $\exists L/k$ конечное неразветвленное : $N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s}$. По предложению 6.3 $\exists L/k$ конечное неразветвленное, такое что $N_{L/\mathbb{Q}_p}(L^*) \subseteq \{p\} \times E_1^{p^s} \Leftrightarrow E_0 \subseteq E_1^{p^s}$. По лемме 6.2 $E_0 \subseteq E_1^{p^s} \Leftrightarrow (p-1)p^s|e_0$. Тем самым, $\exists L/k$ конечное неразветвленное : $\zeta_{p^{s+1}} \in L \Leftrightarrow (p-1)p^s|e_0$. □

7. Заключение. Результаты, полученные в работе, можно применить для оценки степени иррегулярности локальных полей, что, в свою очередь, в дальнейшем дает возможность получить оценки на различные инварианты группы Галуа расширений, как, например, высшие группы ветвления.

В случае формальных модулей информацию об изменении или не изменении степени иррегулярности расширения (по сравнению с нижним полем) можно использовать при описании базиса группы точек формального модуля расширения через элементы нижнего поля. Для неразветвленного расширения, сохраняющего степень иррегулярности, и формальных групп Любина — Тейта этот результат получен в работе [4]. Для многочленных формальных групп удается обобщить результат о вполне регулярности формального модуля с заменой p на p^{s+1}, но доказательство идет по другому пути — через мультипликативный случай.

Литература

1. *Боревич З. И.* О регулярных локальных полях // Вестн. Ленингр. ун-та. 1962. Вып. 1. С. 142–145.

2. *Касселс Дж., Фрёлих А.* Алгебраическая теория чисел. 1969.

3. *Востоков С. В., Некрасов И. И.* Формальный модуль Любина — Тейта в циклическом неразветвленном p-расширении как модуль Галуа // Зап. научн. сем. ПОМИ. 2014. Т. 430. Р. 61–66.

4. *Власьев С. М., Востоков С. В., Горшков А. А.* Регулярные формальные модули в одномерных локальных полях // Вестн. С.-Петерб. ун-та. Сер. 1. Математика. Механика. Астрономия. 2016. Т. 3 (61). Вып. 4. С. 544–551. https://doi.org/10.21638/11701/spbu01.2016.403

Статья поступила в редакцию 15 мая 2020 г.;
после доработки 17 июня 2020 г.;
рекомендована в печать 18 июня 2020 г.

Контактная информация:

Власкина Наталья Константиновна — аспирант; nkvlaskina@yandex.ru
Востоков Сергей Владимирович — д-р физ.-мат. наук, проф.; sergei.vostokov@gmail.com
Питаль Петр Николаевич — ассистент; pital.petya@yandex.ru
Цыбышев Алексей Евгеньевич — аспирант; emperortsy@gmail.com

Regular formal modules in local fields and irregularly degree*

N. K. Vlaskina[1], *S. V. Vostokov*[1], *P. N. Pital'*[1], *A. E. Tsybyshiev*[2]

[1] St. Petersburg State University, 7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation
[2] St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, 27, nab. r. Fontanki, St. Petersburg, 191029, Russian Federation

*Research is supported by the Russian Science Foundation (grant no. 16-11-10200).

For citation: Vlaskina N. K., Vostokov S. V., Pital' P. N., Tsybyshiev A. E. Regular formal modules in local fields and irregularly degree. *Vestnik of Saint Petersburg University. Mathematics. Mechanics. Astronomy*, 2020, vol. 7 (65), issue 4, pp. 588–596.
https://doi.org/10.21638/spbu01.2020.402 (In Russian)

In this paper we investigate the irregular degree of finite not ramified local field extantions with respect to a polynomial formal group and in the multiplicative case. There was found necessary and sufficient conditions for the existence of primitive roots of p^s power from 1 and (endomorphism $[p^s]_{F_m}$) in L-th unramified extension of the local field K (for all positive integer s). These conditions depend only on the ramification index of the maximal abelian subextension of the field K $K_a/\mathbb{Q}_p$.

Keywords: regular formal modules, formal modules, formal groups, local fields.

References

1. Borevich Z. I., "About regular local fields", *Vestn. of Leningrad Univ.*, 142–145 (1962). (In Russian)

2. Cassels J. W. S., Frohlich A., *Algebraic Number Theory* (Academic Press, 1969).

3. Vostokov V., Nekrasov I. I., "Lubin — Tate formal module in a cyclic unramified p-extension as Galois module", *J. Math. Sci. (N. Y.)* **219**(3), 375–379 (2016). https://doi.org/10.1007/s10958-016-3113-6

4. Vlassiev S. M., Vostokov S. V., Gorshkov A. A., "Regular formal modules in onedimensional local fields", *Vestnik St. Petersb. Univ. Math.* **49**, 313–319 (2016). https://doi.org/10.3103/S1063454116040142

Received: May 15, 2020
Revised: June 17, 2020
Accepted: June 18, 2020

Authors' information:

Natalya K. Vlaskina — nkvlaskina@yandex.ru
Sergei V. Vostokov — sergei.vostokov@gmail.com
Pital' N. Petr — pital.petya@yandex.ru
Aleksey E. Tsybyshiev — emperortsy@gmail.com