Math-Net.Ru

Общероссийский математический портал

Д. Д. Киселев, Явные вложения конечных абелевых p -групп в группу $\mathcal{J}(\mathbb{F}_p)$, *Матем. заметки*, 2015, том 97, выпуск 1, 74–79

DOI: <https://doi.org/10.4213/mzm10473>

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: 54.205.225.156

26 апреля 2023 г., 11:38:28

Явные вложения конечных абелевых p -групп в группу $\mathcal{J}(\mathbb{F}_p)$

Д. Д. Киселев

Для каждой конечной абелевой p -группы построено ее явное вложение в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$.

Библиография: 4 названия.

DOI: 10.4213/mzm10473

1. Введение. Пусть k – коммутативное кольцо с единицей. Рассмотрим множество $\mathcal{J}(k)$ формальных степенных рядов относительно переменной x с коэффициентами в кольце k , причем коэффициент при x ряда $f(x) \in \mathcal{J}(k)$ равен единице. Более формально,

$$\mathcal{J}(k) = \left\{ f(x) \in k[[x]] \mid f(x) = x + \sum_{n=2}^{\infty} a_n x^n \right\}. \quad (1.1)$$

На множестве $\mathcal{J}(k)$ можно ввести бинарную операцию: по определению $(f * g)(x) = f(g(x))$; такое определение корректно, так как ряд $g(x) \in \mathcal{J}(k)$ не содержит свободного члена. Впервые ряды такого вида рассмотрел Дженнингс, который в своей работе [1] установил, что относительно так введенной операции $\mathcal{J}(k)$ становится группой, а также показал ряд общих (не зависящих от выбора коммутативного кольца k с единицей) свойств.

В случае $k = \mathbb{F}_p$ группа $\mathcal{J}(\mathbb{F}_p)$ обладает рядом интересных свойств, самым важным из которых, по-видимому, является универсальность: любая про- p -группа счетного ранга изоморфно вкладывается в $\mathcal{J}(\mathbb{F}_p)$. Этот результат был впервые установлен Каминой в [2; следствие 2]. Из этого результата следует, что произвольная конечная p -группа допускает изоморфное вложение в группу $\mathcal{J}(\mathbb{F}_p)$. Однако, доказательство наличия такого вложения даже для абелевых p -групп весьма далеко от конструктивного. И. К. Бабенко в своем обзоре (см. [3; замечание 4.11]) отмечает, что даже явные вложения групп Z_{p^2} и $Z_p \times Z_p$ в $\mathcal{J}(\mathbb{F}_p)$ неизвестны! В то же время вложение группы Z_p в $\mathcal{J}(\mathbb{F}_p)$ строится очевидным образом: надо взять ряд $f(x) = x/(1-x)$, который имеет порядок p .

В данной работе мы дадим конструкцию явных вложений произвольной конечной абелевой p -группы в группу $\mathcal{J}(\mathbb{F}_p)$.

2. Обозначения. Если X – некоторое множество, то символ $\langle X \rangle$ обозначает группу, порожденную множеством X ; Z_m – циклическая группа порядка m ; R^* – группа обратимых элементов кольца R с единицей; если k – некоторое поле, то $\bar{k}$ обозначает переход к некоторому сепарабельному алгебраическому замыканию.

3. Прежде всего нам понадобится отождествить группу $\mathcal{J}(\mathbb{F}_p)$ с некоторой подгруппой в группе автоморфизмов локального поля $\mathbb{F}_p((t))$. С этой целью заметим, что всякий элемент $g \in \text{Aut } \mathbb{F}_p((t))$ является непрерывным относительно естественно-го показательного нормирования $\nu_t(\cdot)$ поля $\mathbb{F}_p((t))$ (за подробностями мы отсылаем читателя к [2; preliminaries]). Из условия непрерывности и групповой структуры нетрудно получить, что тогда, во-первых, элемент $g \in \text{Aut } \mathbb{F}_p((t))$ вполне определяется своим значением на униформизирующей t , а, во-вторых, t^g является степенным рядом относительно переменной t , причем $\nu_t(t^g) = 1$. Рассмотрим в группе $\text{Aut } \mathbb{F}_p((t))$ подгруппу $\mathcal{J}$ вида

$$\mathcal{J} = \left\{ g \in \text{Aut } \mathbb{F}_p((t)) \mid t^g = t + \sum_{n=2}^{\infty} a_n t^n \right\}. \quad (3.1)$$

Группа $\mathcal{J}$ естественным образом отождествляется с группой $\mathcal{J}(\mathbb{F}_p)$ с помощью (1.1) и (3.1) (переменная t “заменяется” на x , и t^g отождествляется тем самым с $f(x)$).

ЗАМЕЧАНИЕ 1. Под “явным вложением” конечной абелевой p -группы типа

$$Z_{p^{s_1}} \times \cdots \times Z_{p^{s_r}}$$

в группу $\mathcal{J}(\mathbb{F}_p)$ будет пониматься следующее: образующие $g_1, \dots, g_r$ соответствующих прямых слагаемых представляют собой степенные ряды, для каждого из которых можно за конечное число шагов вычислить частичную сумму сколь угодно высокой степени. Тем самым, наша формализация термина “явный” вполне отвечает здравому смыслу.

4. Расширения Любина–Тейта. Нам понадобится явное описание максимального абелева вполне разветвленного расширения поля $\mathbb{F}_p((t))$. Такое описание (для произвольных одномерных локальных полей) было впервые дано в работе [4] с помощью указания так называемых *расширений Любина–Тейта*, играющих ту же роль, что и круговые расширения поля рациональных чисел в теореме Кронекера–Вебера.

Рассмотрим многочлен $f(x) = x^p + tx$ как элемент кольца $\mathbb{F}_p[t][x]$. Положим $f^{(0)}(x) := x$ и, индуктивно, $f^{(n)}(x) := f(f^{(n-1)}(x))$ для произвольного натурального n . Нетрудно заметить, что множества $W_{f,n}$ корней многочлена $f^{(n)}(x)$ в фиксированном алгебраическом замыкании $\overline{\mathbb{F}_p((t))}$ поля $\mathbb{F}_p((t))$ вложены друг в друга: $W_{f,n} \subset W_{f,n+1}$ для любого натурального n . Если положить $k_n := \mathbb{F}_p((t))(W_{f,n})$ для $n \in \mathbb{N}$, а $k_0 := \mathbb{F}_p((t))$, то расширение k_n/k_0 является вполне разветвленным расширением Галуа степени $(p-1)p^{n-1}$ с абелевой группой Галуа, изоморфной группе обратимых элементов кольца $\mathbb{F}_p[[t]]/(t^n)$. При этом, если t_n – корень многочлена $f^{(n)}(x)$, являющийся униформизирующей поля k_n , то элемент $t_{n-1} = f(t_n)$ – униформизирующая поля k_{n-1} при $n > 1$. При этом также $t = -(f^{n-1}(t_n))^{p-1}$.

Положим

$$W_{f,\infty} := \bigcup_{n=1}^{\infty} W_{f,n}, \quad k_{\infty} := k_0(W_{f,\infty}).$$

Оказывается, что расширение k_{∞}/k_0 является абелевым вполне разветвленным расширением Галуа, композит которого с максимальным неразветвленным расширением поля k_0 дает максимальное абелево расширение поля k_0 ; при этом k_{∞} не зависит¹

¹Всюду далее под $f(x)$ мы будем поэтому понимать именно многочлен $x^p + tx$.

от выбора униформизирующей поля k_0 и от выбора многочлена $f(x)$: в качестве $f(x)$ можно даже взять любой элемент кольца $\mathbb{F}_p[[t]][[x]]$, удовлетворяющий свойствам

$$\begin{aligned} f(x) &\equiv x^p \pmod{t}, \\ f(x) &\equiv tx \pmod{\deg \geq 2}. \end{aligned}$$

В частности, всякое конечное абелево вполне разветвленное расширение поля k_0 содержится в расширении k_n/k_0 для некоторого n . Расширение k_n/k_0 называется *расширением Любина–Тейта*.

Для каждого $a \in \mathbb{F}_p[[t]]^*$ существует и притом единственный формальный ряд $[a]_f(x) \in \mathbb{F}_p[[t]][[x]]$, обладающий свойствами

$$\begin{aligned} [a]_f(x) &\equiv ax \pmod{\deg \geq 2}, \\ f([a]_f(x)) &= [a]_f(f(x)). \end{aligned}$$

Для $u \in \mathbb{F}_p[[t]]^*$ символ Артина $\theta(u) = (u, k_\infty/k_0)$ задается явно:

$$y^{\theta(u)} := [u^{-1}]_f(y) \quad \text{для всех } y \in W_{f,\infty}.$$

5. Явные конструкции. Для начала нам будет необходимо вычислить для каждого $a \in \mathbb{F}_p[[t]]^*$ ряд $[a]_f(x)$.

ЛЕММА 1. Пусть $h(t) \in \mathbb{F}_p[[t]]^*$, $f(x) = x^p + tx$. Тогда

$$[h(t)]_f(x) = h(t)x + \sum_{n=1}^{\infty} a_{p^n}(t)x^{p^n},$$

где

$$a_{p^{n+1}}(t) := \frac{a_{p^n}(t)^p - a_{p^n}(t)}{t^{p^n} - t}, \quad n \in \mathbb{N}, \quad a_p(t) := \frac{h(t)^p - h(t)}{t^p - t}.$$

ДОКАЗАТЕЛЬСТВО. Мы покажем, что $\psi(x) := [h(t)]_f(x)$ можно определить индуктивно:

$$\psi(x) = \psi_r(x) + (\deg \geq \deg \psi_r + 1),$$

где $\psi_r(x)$ – уже определенный (и притом однозначно) многочлен степени не выше r , удовлетворяющий условиям

$$\begin{aligned} \psi_r(x) &\equiv h(t)x \pmod{\deg \geq 2}, \\ f(\psi_r(x)) &\equiv \psi_r(f(x)) \pmod{\deg \geq r+1}. \end{aligned}$$

Положим $\psi_1(x) := h(t)x$. Имеем

$$f(\psi_1(x)) - \psi_1(f(x)) = h(t)^p x^p + th(t)x - h(t)x^p - h(t)tx \equiv 0 \pmod{\deg \geq 2}.$$

Пусть $\psi_r(x)$ уже определено. Тогда в силу единственности $\psi_{r+1}(x) = \psi_r(x) + Q(x)$, где $Q(x)$ – моном степени $\deg(\psi_r(x)) + 1$. Легко видеть, что надо положить

$$Q(x) \equiv \frac{f(\psi_r(x)) - \psi_r(f(x))}{t^{r+1} - t} \pmod{\deg \geq r+2},$$

причем $t \mid (f(\psi_r(x)) - \psi_r(f(x)))$, так что $\psi_{r+1}(x) \in \mathbb{F}_p[[t]][x]$.

Заметим теперь, что

$$f(h(t)x) - h(t)f(x) = h(t)^p x^p - h(t)x^p,$$

поэтому приближение $\psi_1(x) = h(t)x$ годится вплоть до степени $p-1$ (в частности, можно положить $\psi_{p-1}(x) := \psi_1(x)$), а $a_p(x) = (h(t)^p - h(t))/(t^p - t)$. Предположив по индукции, что

$$[h(t)]_f(x) = h(t)x + \sum_{m=1}^{n-1} a_{p^m}(t)x^{p^m} + (\deg \geq p^{n-1} + 1),$$

причем коэффициенты $a_{p^m}(t)$ вычисляются по формулам, заявленным в формулировке леммы, докажем, что

$$[h(t)]_f(x) = h(t)x + \sum_{m=1}^n a_{p^m}(t)x^{p^m} + (\deg \geq p^n + 1),$$

где $a_{p^n}(t) = (a_{p^{n-1}}(t)^p - a_{p^{n-1}}(t))/(t^{p^n} - t)$.

Заметим, что в поведении разности $f(\psi_r(x)) - \psi_r(f(x))$ для $r = p^{n-1} + 1, \dots, p^n - 1$ нам достаточно отслеживать коэффициент при старшем мономе (это следует из определения многочленов $\psi_k(x)$). Так как $f(x)$ — многочлен степени p , то старший моном указанной разности будет иметь степень p^n , откуда $\psi_r(x) = \psi_{p^{n-1}}(x)$ для всех $r = p^{n-1} + 1, \dots, p^n - 1$. Теперь уже ясно, что коэффициент $a_{p^n}(t)$ имеет указанный выше вид. Лемма доказана.

Пусть по-прежнему $k_0 = \mathbb{F}_p((t))$, $k_n = k_0(W_{f,n})$, а t_i — такой простой элемент поля k_i , что $t_i = f(t_{i+1})$ для $i = 1, \dots, n-1$. Тогда

$$t = -t_1^{p-1} = -(f^{(n-1)}(t_n))^{p-1}.$$

ЛЕММА 2. *Элемент t явно выражается в виде степенного ряда относительно переменной t_n .*

ДОКАЗАТЕЛЬСТВО. Так как $f(x) = x^p + tx$, то t выражается через t_n в виде многочлена, коэффициенты которого лежат в $\mathbb{F}_p[t]$, причем коэффициент при $t_n^{(p-1)p^{n-1}}$ лежит в $\mathbb{F}_p$, а остальные коэффициенты не имеют свободного члена. Иными словами

$$t = -t_n^{(p-1)p^{n-1}} + \gamma(t, t_n), \quad (5.1)$$

где γ — многочлен от t_n с коэффициентами в $\mathbb{F}_p[t]$, не имеющими свободного члена.

Исходя из представления

$$t = \sum_{k=(p-1)p^{n-1}}^{\infty} a_k t_n^k, \quad (5.2)$$

где $a_k \in \mathbb{F}_p$ для всех k , а также из (5.1), можно получить систему нелинейных алгебраических уравнений на коэффициенты $\{a_k\}_{k=(p-1)p^{n-1}}^{\infty}$, каждое уравнение которой имеет лишь конечное число неизвестных. Покажем что такая система будет иметь единственное решение, лежащее в $\mathbb{F}_p^{\infty}$. В самом деле, при подстановке вместо t степенного ряда (5.2) с неопределенными коэффициентами в правую часть (5.1) мы получим конечную сумму степенных рядов, каждый ряд которой есть результат

возведения ряда (5.2) в некоторую натуральную степень и умножения полученного ряда на t_n в некоторой натуральной степени; также в этой сумме будет слагаемое $-t_n^{(p-1)p^{n-1}}$.

Однако, если ряд (5.2) возвести в натуральную степень, то получится ряд, в котором q -й коэффициент является многочленом от переменных $\{a_k\}_{k=(p-1)p^{n-1}}^q$, т.е. многочленом от неопределенных коэффициентов ряда (5.2) с номерами, не превосходящими q . Поэтому сравнение коэффициентов в (5.1) при t_n^k даст слева a_k ; в правой же части будет конечная сумма степенных рядов вида $\sum_{q \geq q_0} c_q t_n^{q+r}$ для некоторого $r \geq 1$, причем c_q полиномиально зависит лишь от $\{a_k\}_{k=(p-1)p^{n-1}}^q$. Чтобы указанный ряд из суммы рядов правой части (5.1) повлиял на определение коэффициента a_k , необходимо выполнение равенства $q + r = k$, но тогда a_k можно однозначно определить по уже известным коэффициентам из последовательности $\{a_s\}_{s=(p-1)p^{n-1}}^\infty$ с номерами, меньшими чем k . Тем самым единственность представления (5.2), удовлетворяющего (5.1), установлена. Более того, доказано, что частичную сумму ряда (5.2) заданной наперед степени можно вычислить за конечное число шагов. Это и означает, что t можно явно выразить через t_n . Лемма доказана.

Дадим теперь с помощью лемм 1 и 2 конструкцию явного вложения произвольной конечной абелевой p -группы в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$.

Фиксируем локальное поле $k_0 = \mathbb{F}_p((t))$ и рассмотрим расширение Любина–Тейта k_n/k_0 , где $k_n = k_0(W_{f,n})$ с группой Галуа, изоморфной $(\mathbb{F}_p[[t]]/(t^n))^*$, а $n = p^m$ для некоторого достаточно большого натурального $m \equiv 0 \pmod{2}$ (позднее мы конкретизируем выбор m). Рассмотрим следующий набор элементов группы $(\mathbb{F}_p[[t]]/(t^n))^*$:

$$g_1 = 1 + t^p + t^{p^2}, \quad g_2 = 1 + t^{p^2} + t^{p^2+1}, \quad \dots, \quad g_{m/2} = 1 + t^{p^{m/2}} + t^{p^{m/2}+1}. \quad (5.3)$$

Элементы $g_1, \dots, g_{m/2}$ в (5.3) записаны, разумеется, по модулю соотношения $t^n = 0$.

ЛЕММА 3. *Элементы $g_1, \dots, g_{m/2}$ порождают с точностью до изоморфизма группу*

$$Z_{p^{m-1}} \times Z_{p^{m-2}} \times \dots \times Z_{p^{m-m/2}}.$$

ДОКАЗАТЕЛЬСТВО. Ясно, что $|g_i| = p^{m-i}$ для каждого $i = 1, \dots, m/2$. Элементы $g_1, \dots, g_{m/2}$ попарно коммутируют, поэтому нам достаточно установить для каждого $i = 2, \dots, m/2$, что элемент g_i не лежит в группе, порожденной элементами $g_1, \dots, g_{i-1}$. Предположим противное. Тогда найдется такое $i = 2, \dots, m/2$, что

$$\prod_{j=1}^k (1 + t^{p^{m-1}} + t^{p^{m-1}+p^{m-s_j}}) = 1 + t^{p^{m-1}} + t^{p^{m-1}+p^{m-i-1}}, \quad (5.4)$$

причем без ограничения общности $2 \leq s_1 < s_2 < \dots < s_k < i+1$. Заметим, что выполнено $t^{p^{m-1}+p^{m-i-1}} \neq 0$, ибо из-за $2 < i+1$ имеем $p^{m-1} + p^{m-i-1} < p^m$.

Далее, в равенстве (5.4) моном $t^{p^{m-1}+p^{m-i-1}}$ в правой части имеет меньшую степень, чем любой моном вида $t^{p^{m-1}+p^{m-s_q}}$, стоящий в некоторой скобке в левой части равенства (5.4). Поэтому чтобы слева в равенстве (5.4) получить моном вида $t^{p^{m-1}+p^{m-i-1}}$, надо выбрать l скобок и взять в каждой из них моном $t^{p^{m-1}}$, а затем из оставшихся скобок взять единицы, после чего привести подобные слагаемые. В итоге получится моном $t^{lp^{m-1}}$ с коэффициентом C_k^l . Поэтому чтобы

получить $t^{p^{m-1}+p^{m-i-1}}$, необходимо требовать выполнения равенства

$$lp^{m-1} = p^{m-1} + p^{m-i-1}. \quad (5.5)$$

(также нужно еще чтобы $C_k^l \equiv 1 \pmod{p}$).

Но если (5.5) выполнено, то

$$1 < l = 1 + \frac{1}{p^i} < 2,$$

что приводит к противоречию. Лемма доказана.

Теперь мы можем установить основной результат работы.

ТЕОРЕМА 1. *Произвольная конечная абелева p -группа вкладывается в группу Дженнинга $\mathcal{J}(\mathbb{F}_p)$, причем искомое вложение допускает явное описание.*

ДОКАЗАТЕЛЬСТВО. Пусть дана произвольная конечная абелева p -группа

$$A \cong Z_{p^{r_1}} \times \cdots \times Z_{p^{r_s}},$$

где $1 \leq r_1 \leq \cdots \leq r_s$. Тогда группа A допускает вложение в группу $(\mathbb{F}_p[[t]]/(t^n))^*$ при $n = p^m$ и $m \geq \max\{2s, 2r_s\}$, $m \equiv 0 \pmod{2}$. В самом деле, согласно лемме 3 элементы $g_1, \dots, g_{m/2}$ из (5.3) порождают в $(\mathbb{F}_p[[t]]/(t^n))^*$ подгруппу, изоморфную

$$Z_{p^{m-1}} \times Z_{p^{m-2}} \times \cdots \times Z_{p^{m-m/2}}.$$

Группа A вкладывается в группу $\langle g_1, \dots, g_{m/2} \rangle$ и, тем самым, в группу $(\mathbb{F}_p[[t]]/(t^n))^*$, причем если $a_1, \dots, a_s$ — образующие группы A , то можно считать $a_i = g_i^{p^{m-i-r_i}}$ для всех $i = 1, \dots, s$.

Группа $(\mathbb{F}_p[[t]]/(t^n))^*$ является группой Галуа расширения $\mathbb{F}_p((t))(W_{f,n})/\mathbb{F}_p((t))$. Такое расширение вполне разветвлено, поэтому если t_n — униформизирующая поля $\mathbb{F}_p((t))(W_{f,n})$, то $\mathbb{F}_p((t))(W_{f,n}) = \mathbb{F}_p((t_n))$. На основании раздела 3 можно утверждать, что группа A вложена в $\mathcal{J}(\mathbb{F}_p)$ (отождествление задано формулами (1.1) и (3.1)).

Заметим, что элементы $g_1, \dots, g_{m/2}$ из (5.3) действуют на униформизирующую t_n следующим образом: для каждого $i = 1, \dots, m/2$ имеем $t_n^{g_i} := [g_i]_f(t_n)$. Леммы 1 и 2 дают искомое конструктивное описание группы A как подгруппы в $\mathcal{J}(\mathbb{F}_p)$. Теорема доказана.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] S. A. Jennings, “Substitution groups of formal power series”, *Canad. J. Math.*, **6** (1954), 325–340.
- [2] R. Camina, “Subgroups of the Nottingham group”, *J. Algebra*, **196**:1 (1997), 101–113.
- [3] И. К. Бабенко, “Алгебра, геометрия и топология группы подстановок формальных степенных рядов”, *УМН*, **68**:1 (2013), 3–76.
- [4] J. Lubin, J. Tate, “Formal complex multiplication in local fields”, *Ann. of Math. (2)*, **81**:2 (1965), 380–387.

Д. Д. Киселев

Всероссийская академия внешней торговли,
г. Москва

E-mail: denmexmath@yandex.ru

Поступило

07.02.2014

Исправленный вариант

12.05.2014