

А. Ф. ИВАНОВ

ОБ АРИФМЕТИКЕ p -РАСШИРЕНИЙ

(Представлено академиком Ю. В. Линником 26 VII 1971)

В работе дается описание и алгоритм построения p -расширений для любых полей характеристики p (и даже конечных полей). В применении же к полям алгебраических функций получается эффективное выражение для символа Артина и полное описание характеров Дирихле степени p^n . Как арифметическое следствие получается эффективная разрешимость «краевой задачи» (Н. Г. Чудаков): построить характер Дирихле, принимающий на заданном конечном наборе простых дивизоров заданные значения (в нашем случае корни степени p^n из единицы).

Наша конструкция p -расширений дается в терминах основного поля и является естественной по отношению к вложениям расширения меньшей степени в большее; язык бесконечных расширений вносит известное единообразие.

Обозначения. K — произвольное поле характеристики p , K_i — циклическое расширение K степени p^i , κ_i^j — вложение $K_i \rightarrow K_j$, $\kappa_i^i \kappa_i^j = \kappa_i^{i+j}$, $\gamma_i^j: G(K_j/K) \rightarrow G(K_i/K)$ — соответствующий κ_i^j гомоморфизм ограничения, $\{\sigma_j\}$ — последовательность порождающих автоморфизмов $G(K_j/K)$ такая, что $\gamma_i^j(\sigma_j) = \sigma_i$; K_∞ — бесконечное p -расширение (любое конечное расширение E/K , $E \subset K_\infty$, циклическое степени p^n), $K_\infty = \varinjlim (\kappa_i^i, K_i)$, $\sigma_\infty = \varinjlim (\gamma_i^j, \sigma_j)$ — порождающий элемент $G(K_\infty/K) \approx Z_p$ над Z_p ; $\mathfrak{p}$ — простой дивизор, $\Sigma_{\mathfrak{p}}$ — его поле вычетов, $r(\mathfrak{p})$ — значение элемента r поля в точке $\mathfrak{p}$, $d\mathfrak{p}$ — его степень; N — натуральное число или ∞ .

Теорема 1. Пусть R — поле алгебраических функций от одной переменной над полем констант $[q]$, $q = p^m$, R_N — его p -расширение, σ_N — порождающий элемент $G(K_N/K)$.

Существует набор элементов $\{r_{p^i}\}_{i=0}^{N-1}$ (для $N = \infty$ это бесконечная последовательность, занумерованная целыми числами i , $i \geq 0$) такой, что

1) совокупность всех полюсов всех r_{p^i} совпадает с множеством ветвящихся в R_N/R дивизоров поля R ;

2) для остальных простых дивизоров $\mathfrak{p}$
$$\mathfrak{p}\left(\frac{R_N}{R}\right) = \sigma_N^{-1} \sum_{i=0}^{N-1} l_i(\mathfrak{p}) p^i, \quad \text{где } 0 \leq \leq l_i(\mathfrak{p}) < p.$$

$l_i(\mathfrak{p}) = F_{i, m d \mathfrak{p}}(r_{p^i}(\mathfrak{p}), \dots, r_{p^i}(\mathfrak{p})), F_{i, m d \mathfrak{p}}$ — полином над $[p]$. (1)

Характер зависимости $F_{i, m d \mathfrak{p}}$ от $s = m d \mathfrak{p}$ таков:

$$F_{0, s}(x) = \text{Sp}_{[p^s]/[p]} x_0, \quad x_0 \in [p^s]; \quad F_{i, s}(x_0, \dots, x_i) = \\ = G_i(S_1(g_v(x)), \dots, S_{p^i}(g_v(x))),$$

где G_i и $\{g_v\}$ — некоторые полиномы, зависящие лишь от i и p (но не от $\mathfrak{p}$ и не от R), а S_j — j -я элементарная симметрическая функция для расширения $[p^s]/[p]$, $S_1 = \text{Sp}_{[p^s]/[p]}$ и т. д.

Замечание. Если множество ветвящихся дивизоров пусто, то $\{r_{p^i}\}$ могут быть выбраны имеющими не более одного полюса.

Теорема 2. Пусть $\{r_{p^i}\}_{i=0}^{N-1}$ — набор элементов из R , $r_1 \neq b^p - b$ для $b \in R$.

Тогда существует p -расширение R_N (степени N , если N конечно) и порождающий автоморфизм σ_N такие, что для всех $\mathfrak{p}$, $v_{\mathfrak{p}}(r_{p^i}) \geq 0 \forall i$, символ Артина $\left(\frac{R_N}{R}\right)$ дается формулой (1).

Конечный и бесконечный случай «согласованы»:

$$\left(\frac{R_n}{\mathfrak{p}}\right) = \gamma_n^N \left(\left(\frac{R_N}{\mathfrak{p}}\right)\right) = (\gamma_n^N(\sigma_N))_{i=0}^{N-1} l_i p^i = \sigma_n^{\sum_{i=0}^{n-1} l_i p^i},$$

что совпадает с (1) для R_n/R . Иными словами, $r_1, \dots, r_{p^{n-1}}$ — набор параметров для R_n/R , о котором говорится в теореме (l_i зависит лишь от i первых элементов набора $\{r_{p^v}\}$). Отметим, что для R_n/R требуется конечное число параметров $\{r_{p^v}\}$, а именно n .

Следствие 1. Для любого характера Дирихле χ степени p^n поля существует набор элементов $r_1, r_p, \dots, r_{p^{n-1}} \in R$, $r_1 \neq b^p - b$ для всех

$b \in R$ такой, что $\chi(\mathfrak{p}) = \exp \left\{ \frac{2\pi i}{p^n} \sum_{i=0}^{n-1} l_i(\mathfrak{p}) p^i \right\}$, где $l_i(\mathfrak{p})$ заданы формулами

(1). Обратно, для любого набора $r_1, \dots, r_{p^{n-1}}$, $r_1 \neq b^p - b$, так определенная функция есть характер Дирихле степени p^n .

Следствие 2. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ — конечный набор дивизоров поля R , $\varepsilon_1, \dots, \varepsilon_s$ — целые p -адические числа. Существуют расширение R_∞/R и изоморфизм $\chi: G(R_\infty/R) \rightarrow Z_p$ такие, что $\chi\left(\left(\frac{R_\infty}{\mathfrak{p}_i}\right)\right) = \varepsilon_i$.

Следствие 2'. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ — конечный набор дивизоров поля R , $\varepsilon'_1, \dots, \varepsilon'_s$ — корни степени p^n из единицы. Существует характер Дирихле χ' поля R , для которого $\chi'(\mathfrak{p}_i) = \varepsilon'_i$.

Формально следствие 2' может быть получено из следствия 2, если положить $\chi' = \psi\chi\left(\left(\frac{R_\infty}{\mathfrak{p}}\right)\right)$, $\varepsilon'_i = \psi(\varepsilon_i)$, где ψ — какой-нибудь непрерывный характер Z_p . Для доказательства этих следствий достаточно заметить, что $F_{i, \text{dmp}}(r_1(\mathfrak{p}), \dots, r_{p^i}(\mathfrak{p})) = \text{Spr}_{\mathfrak{p}/[p]}(r_{p^i}(\mathfrak{p})) + G(r_1(\mathfrak{p}), \dots, r_{p^{i-1}}(\mathfrak{p}))$, а $\text{Spr}_{\mathfrak{p}/[p]}$ — эпиморфизм.

Применяемая конструкция, из которой легко получается конструкция (1), стр. 201—202, такова. Пусть сначала имеется K_N/K и σ_N . Применяя теорему Гильберта или же используя матричную запись $(\sigma_N - 1)$ (ср. (2)), строим цепочку элементов ω_i : $\omega_0 = 1$, $(\sigma_N - 1)\omega_i = \omega_{i-1}$, $i = 1, \dots, p^{N-1}$. При этом ω_{p^v} порождает K_{v+1} , а ω_j , $p^v \leq j < p^{v+1}$, лежат в том же поле. Действие степеней σ на ω_i определяется самой рекурренцией ω_i для

$$k = \sum_{i=0}^{N-1} l_i p^i$$

$$\sigma_N^k(\omega_i) = \sigma_v^k(\omega_i) = \sum_{l=\max(i-k, 1)}^i C_k^{i-l} \omega_l + l_{v-1}, \quad (2)$$

где $p^{v-1} \leq i < p^v$.

Вводятся также элементы $t_i = \omega_i^p - \omega_i$; для них также $(\sigma_N - 1)t_i = t_i - 1$, а значит, существует последовательность $\{r_i\}$, $r_i \in K$, такая, что

$$t_i = r_1 \omega_{i-1} + r_2 \omega_{i-2} + \dots + r_i. \quad (3)$$

Оказывается, основную роль играют r_i с $i = p^v$, $v = 0, \dots, N-1$. По ним можно построить некоторое p -расширение K_N' . Именно, $K_1' = K(\omega_1)$, где ω_1 — корень $\omega_1^p - \omega_1 = r_1$; $\sigma_1 \omega_1 = \omega_1 + 1$. Используя матричную запись $(\sigma_1 - 1)$ в базисе $\{\omega_1^v\}$, восстанавливаем $\omega_2, \dots, \omega_{p-1}$, что дает $r_2, \dots, r_{p-1}$. Определим ω_p уравнением $\omega_p^p - \omega_p = r_1 \omega_{p-1} + \dots + r_p$. Пусть $\tilde{\sigma}$ — продолжение σ_1 на $K(\omega_1, \omega_2)$. Так как $(\tilde{\sigma} \omega_p - \omega_p)^{p-1} (\tilde{\sigma} \omega_p - \omega_p) = t_{p-1} = \omega_{p-1}^p - \omega_{p-1}$, то $\tilde{\sigma} \omega_p = \omega_p + \omega_{p-1} + i$, $i \in [p]$, и полагаем $\sigma_2 =$

$= \delta^{(p-1)p+1}$. Теперь $\sigma_2 \omega_p = \omega_p + \omega_{p-1}$, (2) выполнено, $\sigma_2|_{K_1} = \sigma_1$, K_2' требуемого типа и т. д.

Такое построение, вообще говоря, неоднозначно. Геометрическая идея «специализации» подсказывает способ сделать его однозначным (каноническим). Именно, предыдущая конструкция проводится для $K^0 = [p](X_0, X_1, \dots)$, в качестве r_{p^i} выбирается $R_{p^i} = X_i$. Достаточно даже на i -ом шаге работать над полем $[p](X_0, \dots, X_{i-1})$. Элементы Ω_j можно выбрать целыми над $[p][X_0, X_1, \dots]$, а тогда $R_j \in [p][X_0, \dots, X_i]$, $p^v \leq j < p^{v+1}$. Автоморфизм Σ_i поля $K_{i,i} = [p](X_0, \dots, X_{i-1}) (\Omega_1, \dots, \Omega_{p^{i-1}})$ продолжается на $K_{i,i}(X_i)$ тем, что $\Sigma_i(X_i) = X_i$; $\kappa_{j,j}^{i,i}$ — очевидные вложения. Положим $K_{i,i}^0 = [p][X_0, \dots, X_{i-1}][\Omega_1, \dots, \Omega_{p^{i-1}}]$. $K_{i,i}^0$ является «универсальным объектом» для K_i/K : существует гомоморфизм $A_i: K_{i,i}^0 \rightarrow K_i$ такой, что $A_i(X_j) = r_{p^j} \in K$, и K_i порождается над K образом A_i ; $\omega_j = A_i(\Omega_j)$; σ_i , определяемый по (2), согласован с Σ_i ; $t_j = A_i(T_j) = A_i(R_i)\omega_1 + \dots, r_j = A_i(R_j)$. Обратно, любое отображение $\alpha_i: (X_0, \dots, X_{i-1}) \rightarrow (r_1, \dots, r_{p^{i-1}})$, $r_1 \neq b^p - b$, $b \in K$, продолжается до $A_i: K_{i,i}^0 \rightarrow \bar{K}$ ($\bar{K}$ — алгебраическое замыкание); если A_i', K_i', σ_i' — другая «специализация», продолжающая α_i , то существует изоморфизм $\theta_i: K_i \rightarrow K_i'$ такой, что $A_i' = \theta_i A_i$, $\sigma_i' = \theta_i \sigma_i \theta_i^{-1}$. (Здесь используется неприводимость образа характеристического многочлена для $\Omega_{p^{i-1}}$ при действии α_i и справедливость (2).) Наконец, эта система объектов и гомоморфизмов выдерживает переход к пределу (для θ_i это следует, благодаря «пиморфности» A_i , из коммутативности диаграмм). Тем самым построен универсальный объект для p -расширений, канонически фиксирующий алгоритм: если зафиксировать $\bar{K}$, то K_N и σ_N определены последовательностью $\{r_{p^i}\}$ однозначно.

Для вычисления символа Артина достаточно сравнить (2) с $\left(\frac{R_n}{p}\right) \omega_{p^{n-1}} - \omega_{p^{n-1}} \equiv \sum_{k=0}^{m \text{ д } p-1} t_{p^{n-1}}^{pk} \pmod{\text{Con}_{R \setminus R_n} p}$; заменяя справа ω_i^{pk} через $\omega_i + \sum_{j=0}^{k-1} t_i^{pj}$,

приходим к сравнению $\sum_{i=1}^{p^{n-1}-1} C_i \omega_i + l_{n-1} \equiv \sum f_i(r) \omega_i + F(r) \pmod{\text{Con } p}$,

откуда действием степеней $(\sigma - 1)$, благодаря инвариантности $\text{Con } p$ при действии σ и рекуррентности для ω_i , получаем $C_i \equiv f_i(r) \pmod{p}$, и значит, $F(r) \equiv l_{n-1} \pmod{p}$, т. е. просто равенство (1). Универсальный характер полинома F следует из того, что $t_i = A(T_i)$.

Утверждение 1) теоремы 1 следует из рассуждений (3) с помощью теоремы Римана — Рока (4).

Из следствия 2 вытекает, что сумма $\sum_{x \bmod p^n} \exp \left\{ \frac{2\pi i}{p^n} f(x) \right\}$, где f — целочисленный полином, может быть выражена через нули L -функции некоторого поля алгебраических функций.

Вся конструкция принимает очень простой вид в терминах алгебраических групп (формальных степенных рядов). При этом символ Артина проциклического p -расширения и характер Дирихле выражаются нормой в поле формальных степенных рядов.

Ленинградское отделение
Математического института им. В. А. Стеклова
Академии наук СССР

Поступило
8 VII 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ Н. Бурбаки, Алгебра. Многочлены и поля. Упорядоченные группы, «Наука», 1965. ² А. Ф. Иванов, Вестн. Ленингр. ун-в., № 1 (в. 1), 30 (1970). ³ H. Hasse, J. Reine u. Angew. Math., 172, 37 (1935). ⁴ К. Шевалле, Введение в теорию алгебраических функций от одной переменной, М., 1959. ⁵ P. Gabriel, Jahresber. d. Deutsch. Math. Verein., 72, Н. 2/3, 116 (1970).