Math-Net.Ru

Общероссийский математический портал

В. Ф. Молчанов, Преобразование Радона на пространстве над кольцом классов вычетов, *Матем. сб.*, 2012, том 203, номер 5, 119–134

DOI: <https://doi.org/10.4213/sm7838>

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: 3.85.7.115

26 апреля 2023 г., 14:15:10

УДК 517.444

В. Ф. Молчанов

Преобразование Радона на пространстве над кольцом классов вычетов

Функции на пространстве размерности N над кольцом $\mathbb{Z}_n$ классов вычетов по модулю n , инвариантные относительно группы $\mathrm{GL}(N, \mathbb{Z}_n)$, образуют коммутативную алгебру относительно свертки. Описывается структура этой алгебры, находятся собственные векторы и собственные числа операторов умножения на элементы этой алгебры. Полученные результаты применяются к решению обратной задачи для преобразования Радона на $\mathbb{Z}_n^N$ по гиперплоскостям.

Библиография: 2 названия.

Ключевые слова: преобразование Радона, кольцо классов вычетов, функция Мёбиуса, алгебры функций.

Функции со значениями в $\mathbb{C}$ на пространстве $\mathbb{Z}_n^N$ ($\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$), инвариантные относительно группы $\mathrm{GL}(N, \mathbb{Z}_n)$, образуют коммутативную алгебру $\mathcal{M}(\mathbb{Z}_n^N)$ относительно свертки. В настоящей работе мы описываем структуру этой алгебры, находим собственные векторы и собственные числа операторов умножения на элементы этой алгебры и применяем полученные результаты к решению обратной задачи для преобразования Радона на $\mathbb{Z}_n^N$ (см. теорему 5.4).

Задача обращения преобразования Радона для проективного пространства над конечным коммутативным кольцом с единицей (в частности, над $\mathbb{Z}_n$) была изучена в работе [1].

§ 1. Пространство над конечным кольцом

Для конечного множества X мы обозначаем через $L(X)$ пространство функций $f(x)$ на X со значениями в $\mathbb{C}$ и через $|X|$ – количество элементов в X . Размерность $L(X)$ равна $|X|$.

Пусть K – конечное коммутативное кольцо, $K^N = K \times \cdots \times K$ – пространство над K размерности N . Пространство $L(K^N)$ есть алгебра (над $\mathbb{C}$) относительно свертки:

$$(f * h)(x) = \sum_{u \in K^N} f(u)h(x - u) = \sum_{v \in K^N} f(x - v)h(v).$$

Пусть δ_z обозначает дельта-функцию, сосредоточенную в точке z : $\delta_z(x) = 1$ при $x = z$, $\delta_z(x) = 0$ при $x \neq z$. Дельта-функции δ_z , $z \in K^N$, образуют базис

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 09-01-00325), АВЦП “Развитие научного потенциала высшей школы” (проекты № 1.1.2.1474 и № 1.1.1.11), ФЦП “Научные и научно-педагогические кадры инновационной России” (проект № 14.740.11.0349).

в $L(K^N)$. Для них свертка означает сложение носителей: $\delta_z * \delta_w = \delta_{z+w}$, так что единицей в алгебре $L(K^N)$ служит дельта-функция $\delta = \delta_0$, сосредоточенная в начале координат.

Пусть $G = \text{GL}(N, K)$ – группа обратимых матриц порядка N над K . Она действует на K^N линейно: $x \mapsto gx$, где $g \in G$, x – вектор (столбец) из K^N . Множество K^N распадается на G -орбиты $A_1, \dots, A_s$. Точка 0 – одна из орбит. Обозначим через $\mathcal{M}(K^N)$ подпространство функций из $L(K^N)$, инвариантных относительно G , т.е. постоянных на G -орбитах. Оно является подалгеброй в $L(K^N)$. В самом деле, если функции f, h принадлежат $\mathcal{M}(K^N)$, т.е. $f(gx) = f(x)$, $h(gx) = h(x)$, $x \in K^N$, $g \in G$, то их свертка тоже обладает этим свойством:

$$\begin{aligned} (f * h)(gx) &= \sum_u f(gx - u)h(u) = \sum_u f(x - g^{-1}u)h(u) \\ &= \sum_v f(x - v)h(gv) = \sum_v f(x - v)h(v) = (f * h)(x). \end{aligned}$$

Дельта-функцию, сосредоточенную на орбите A_i (характеристическую функцию этой орбиты), будем обозначать тем же символом A_i . Свертку $A_i * A_j$ будем записывать в виде $A_i A_j$, она разлагается по дельта-функциям A_k :

$$A_i A_j = \sum_{k=1}^s c_{ij}^k A_k.$$

Структурные константы c_{ij}^k алгебры $\mathcal{M}(K^N)$ равны кратностям точек из A_k в арифметической сумме $A_i + A_j$ множеств A_i и A_j . Это следует из того, что группа G сохраняет сложение: $g(x + y) = gx + gy$.

§ 2. Преобразование Радона

Введем в K^N билинейную форму $\langle x, y \rangle = x_1 y_1 + \dots + x_N y_N$. Назовем *гиперплоскостью* в K^N множество h точек x , удовлетворяющих уравнению $\langle a, x \rangle = c$, где координаты $a_1, \dots, a_N$ вектора a взаимно просты, т.е. не имеют общих делителей, отличных от 1. Обозначим через H множество всех гиперплоскостей и через H_0 – множество всех гиперплоскостей, проходящих через начало координат: $\langle a, x \rangle = 0$.

Преобразование Радона $\mathcal{R}: L(K^N) \rightarrow L(H)$ сопоставляет функции f из $L(K^N)$ ее “интегралы” по гиперплоскостям h :

$$(\mathcal{R}f)(h) = \sum_{x \in h} f(x).$$

Сопряженный оператор $\mathcal{R}^*: L(H) \rightarrow L(K^N)$ дается формулой

$$(\mathcal{R}^*F)(x) = \sum_{x \in h} F(h).$$

Оператор $S = \mathcal{R}^* \mathcal{R}$ действует в $L(K^N)$:

$$(Sf)(x) = \sum_{y \in K^N} S(x, y) f(y),$$

где $S(x, y)$ равно количеству гиперплоскостей h , проходящих через точки x и y (для $x = y$ это количество гиперплоскостей h , проходящих через x), так что матрица $S(x, y)$ оператора S есть матрица инцидентий. Она инвариантна относительно сдвигов: $S(x+u, y+u) = S(x, y)$, поэтому зависит только от разности: $S(x, y) = T(x-y)$. Для каждой точки x число $T(x)$ есть количество гиперплоскостей из H_0 , проходящих через эту точку. Действие группы G на K^N порождает сопряженное действие группы G на H_0 : для соответствующих векторов a это действие есть $a \mapsto (g')^{-1}a$, где штрих означает матричное транспонирование. Поскольку группа G сохраняет инцидентность, функция $T(x)$ инвариантна относительно G , т.е. она входит в $\mathcal{M}(K^N)$.

Предположим, что оператор S обратим. Тогда $\mathcal{R}$ обладает левым обратным $L = S^{-1}\mathcal{R}^*$. Матрица $\hat{S}(x, y)$ оператора S^{-1} тоже зависит только от разности: $\hat{S}(x, y) = \hat{T}(x-y)$. Равенство $S^{-1}S = E$ на языке матриц имеет вид

$$\sum_{u \in K^N} \hat{T}(x-u)T(u-y) = \delta(x-y).$$

Полагая $y = 0$, получим $\sum \hat{T}(x-u)T(u) = \delta(x)$, или $\hat{T} * T = \delta$, т.е. $\hat{T}$ есть элемент алгебры $\mathcal{M}(K^N)$, обратный к T в смысле свертки.

Это сводит задачу об обращении преобразования Радона к нахождению обратного элемента $T^{-1} = \hat{T}$ для T в алгебре $\mathcal{M}(K^N)$.

§ 3. Функции Эйлера

Назовем *функциями Эйлера* $\varphi_R(n)$, $R \in \mathbb{Z}$, следующие функции натурального переменного n . Разложим натуральное число n на простые множители:

$$n = p_1^{k_1} \cdots p_s^{k_s}, \quad (3.1)$$

где $p_1, \dots, p_s$ – различные простые числа, $k_1, \dots, k_s$ – положительные целые числа. Множители $m_i = p_i^{k_i}$ называются примарными множителями числа n . Таким образом, вместе с (3.1) мы имеем следующее разложение на множители:

$$n = m_1 \cdots m_s. \quad (3.2)$$

Мы полагаем

$$\varphi_R(n) = n^R \left(1 - \frac{1}{p_1^R}\right) \cdots \left(1 - \frac{1}{p_s^R}\right), \quad n \geq 2, \quad (3.3)$$

$$\varphi_R(1) = 1. \quad (3.4)$$

Функции $\varphi_R(n)$ – мультипликативные функции:

$$\varphi_R(n) = \varphi_R(m_1) \cdots \varphi_R(m_s).$$

При $R = 1$ мы получаем классическую функцию Эйлера $\varphi(n)$, она указывает количество натуральных чисел $< n$, взаимно простых с n . Отметим, что

$$\sum_{d|n} \varphi_R(d) = n^R. \quad (3.5)$$

Напомним (см. [2]) формулу обращения Мёбиуса для функции Мёбиуса $\mu(n)$. Последняя определяется так: $\mu(1) = 1$, $\mu(n) = (-1)^s$ при $k_1 = \dots = k_s = 1$ и $\mu(n) = 0$, если какой-либо k_i больше единицы (см. (3.1)). Пусть для функций $f(n)$ и $g(n)$ выполняется условие

$$f(n) = \sum_{d|n} g(d),$$

тогда можно обратить это соотношение и выразить g через f :

$$g(n) = \sum_{d|n} f\left(\frac{n}{d}\right);$$

из второго соотношения также следует первое.

Формула суммирования (3.6) (“формула свертки”) и ее обращение (3.7) с помощью функции Мёбиуса μ играют решающую роль в вычислении коэффициентов в § 5.

ТЕОРЕМА 3.1. Пусть R, L – целые числа, пусть c, d – делители числа n . Тогда

$$\sum_{d|c} d^{R-L} \varphi_{R-L}\left(\frac{n}{d}\right) \varphi_L(d) = \varphi_R(n) \frac{\varphi_{R-L}(n/c)}{\varphi_R(n/c)}, \quad (3.6)$$

$$\varphi_R(n) \sum_{c|d} \mu\left(\frac{d}{c}\right) \frac{\varphi_{R-L}(n/c)}{\varphi_R(n/c)} = d^{R-L} \varphi_{R-L}\left(\frac{n}{d}\right) \varphi_L(d). \quad (3.7)$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3.1. В силу теоремы обращения Мёбиуса достаточно доказать одну из формул (3.6) и (3.7), удобнее взять (3.7). В силу мультипликативности входящих в эти формулы функций достаточно доказать (3.7) для примарного $n = m = p^k$. Пусть $d = m/p^\alpha$, $c = m/p^r$, тогда надо доказать формулу

$$\varphi_R(m) \sum_{r \geq \alpha} \mu(p^{r-\alpha}) \frac{\varphi_{R-L}(p^r)}{\varphi_R(p^r)} = \left(\frac{m}{p^\alpha}\right)^{R-L} \varphi_{R-L}(p^\alpha) \varphi_L\left(\frac{m}{p^\alpha}\right). \quad (3.8)$$

Для краткости обозначим $1 - p^{-L} = u$, $1 - p^{-R+L} = v$, $1 - p^{-R} = w$. Из определения функций Эйлера следует, что правая часть (3.8) равна

$$\begin{cases} m^R u, & \alpha = 0, \\ m^R u v p^{-L\alpha}, & 0 < \alpha < k, \\ m^R v p^{-Lk}, & \alpha = k, \end{cases} \quad (3.9)$$

дробь $\varphi_R(m) \varphi_{R-L}(p^r) / \varphi_R(p^r)$ из левой части (3.8) равна

$$\begin{cases} m^R w, & r = 0, \\ m^R v p^{-Lr}, & 0 < r \leq k. \end{cases} \quad (3.10)$$

Левая часть (3.8) фактически состоит из двух слагаемых с $r = \alpha$ и $r = \alpha + 1$ при $0 \leq \alpha < k$ и одного слагаемого с $r = \alpha$ при $\alpha = k$, коэффициенты μ соответственно равны $+1$, -1 и $+1$. С помощью (3.9) и (3.10) убеждаемся, что левая и правая части (3.8) совпадают.

§ 4. Алгебра $\mathcal{M}(\mathbb{Z}_n^N)$

Кольцо $\mathbb{Z}_n$ состоит из чисел $0, 1, 2, \dots, n-1$, арифметические действия производятся по модулю n . Мы рассматриваем N -мерное ($N \geq 2$) пространство $\mathbb{Z}_n^N$ над кольцом $\mathbb{Z}_n$. Для делителя $d \in \{1, 2, \dots, n\}$ числа n обозначим через A_d множество точек $x = (x_1, \dots, x_N)$ из $\mathbb{Z}_n^N$, для которых наибольший общий делитель координат $x_1, \dots, x_N$ равен d . В частности, A_n состоит из одной точки 0 (начало координат). Множество A_d с $d < n$ содержит, в частности, точки $(d, 0, \dots, 0)$, $(0, d, 0, \dots, 0)$, $\dots$.

ТЕОРЕМА 4.1. *Количество точек в A_d есть*

$$|A_d| = \varphi_N\left(\frac{n}{d}\right). \quad (4.1)$$

В самом деле, достаточно показать, что $|A_1| = \varphi_N(n)$. Последнее утверждение доказывается аналогично формуле (3.3) для классической функции Эйлера $\varphi_1(n)$.

ТЕОРЕМА 4.2. *Каждое из множеств A_d – орбита группы $G = \text{GL}(N, \mathbb{Z}_n)$ на множестве $\mathbb{Z}_n^N$, так что количество орбит равно количеству делителей числа n , т.е. равно $(k_1 + 1) \cdots (k_s + 1)$.*

Приведем формулу (хотя она нам и не понадобится) для порядка группы G :

$$|G| = n^{N(N-1)/2} \varphi_1(n) \varphi_2(n) \cdots \varphi_N(n).$$

Для краткости обозначим алгебру $\mathcal{M}(\mathbb{Z}_n^N)$ через $\mathcal{M}(n)$. Базис в этой алгебре образуют дельта-функции A_d , $d \mid n$ (как и в § 1, мы обозначаем дельта-функцию, сосредоточенную на некотором множестве, тем же символом, что и само множество). Единицей E служит элемент A_n . Умножение базисных элементов A_d мы определим ниже (см. теорему 4.8).

Перейдем к другому базису $\{B_d\}$ в $\mathcal{M}(n)$:

$$B_d = \sum_{d \mid c} A_c. \quad (4.2)$$

Обратный переход дается функцией Мёбиуса:

$$A_d = \sum_{d \mid c} \mu\left(\frac{c}{d}\right) B_c. \quad (4.3)$$

ТЕОРЕМА 4.3. *Количество точек в множестве B_d есть*

$$|B_d| = \left(\frac{n}{d}\right)^N. \quad (4.4)$$

В самом деле, множество B_d состоит из точек $x = (x_1, \dots, x_N)$, координаты x_i которых делятся на d , т.е. $B_d = d \cdot \mathbb{Z}_n^N$. Заметим, что формула (4.4) следует также из (4.2), (4.1) и (3.5) с $R = N$.

ТЕОРЕМА 4.4. Умножение базисных элементов B_d алгебры $\mathcal{M}(n)$ дается следующей формулой:

$$B_d B_c = \left(\frac{n}{[d, c]} \right)^N B_{(d, c)}, \quad (4.5)$$

где $[d, c]$ и (d, c) обозначают наименьшее общее кратное и наибольший общий делитель чисел d и c соответственно.

ДОКАЗАТЕЛЬСТВО. Возьмем в $\mathbb{Z}_n$ два подмножества $d \cdot \mathbb{Z}_n$ и $c \cdot \mathbb{Z}_n$ (подгруппы относительно сложения) чисел, делящихся на d и на c соответственно, и сложим каждый элемент из первой подгруппы с каждым элементом из второй. Мы получим подгруппу $(d, c) \cdot \mathbb{Z}_n$ чисел, делящихся на (d, c) , причем каждое число получается $n/[d, c]$ раз. Отсюда следует теорема.

Вспомним разложения (3.1), (3.2) и возьмем примарный множитель $m = p^k$ ($m = m_i$, $p = p_i$, $k = k_i$). Элементы

$$B_n, B_{n/p}, B_{n/p^2}, \dots, B_{n/p^k} \quad (4.6)$$

порождают в $\mathcal{M}(n)$ подалгебру. Назовем ее *примарной* подалгеброй и обозначим $\mathcal{M}(n, m)$. По (4.5) умножение ее базисных элементов дается формулой

$$B_{n/p^\alpha} B_{n/p^\beta} = p^{\beta N} B_{n/p^\alpha}, \quad \alpha \geq \beta. \quad (4.7)$$

ТЕОРЕМА 4.5. Алгебра $\mathcal{M}(n)$ разлагается в тензорное произведение своих примарных подалгебр:

$$\mathcal{M}(n) = \mathcal{M}(n, m_1) \otimes \dots \otimes \mathcal{M}(n, m_s), \quad (4.8)$$

так что $\mathcal{M}(n)$ изоморфна тензорному произведению:

$$\mathcal{M}(n) \cong \mathcal{M}(m_1) \otimes \dots \otimes \mathcal{M}(m_s).$$

ДОКАЗАТЕЛЬСТВО. Из (4.5) следует, что всякий базисный элемент B_d разлагается в произведение базисных элементов, лежащих в примарных подалгебрах. А именно, пусть $d = n/(p_1^{\alpha_1} \dots p_s^{\alpha_s})$, тогда

$$B_d = B_{n/p_1^{\alpha_1}} \dots B_{n/p_s^{\alpha_s}}. \quad (4.9)$$

Это доказывает (4.8). Изоморфизм $\mathcal{M}(n, m) \cong \mathcal{M}(m)$ устанавливается с помощью соответствия $B_{n/p^\alpha} \longleftrightarrow C_{m/p^\alpha}$, где C_r обозначает дельта-функцию в $\mathcal{M}(m)$ с носителем $r \cdot \mathbb{Z}_m^N$.

Нормируем базис $\{B_d\}$: положим

$$\tilde{B}_d = \left(\frac{n}{d} \right)^{-N} B_d. \quad (4.10)$$

Умножение элементов этого базиса дается формулой

$$\tilde{B}_d \tilde{B}_c = \tilde{B}_{(d, c)},$$

так что он состоит из идемпотентов. Для нормированного базиса

$$\tilde{B}_n, \tilde{B}_{n/p}, \tilde{B}_{n/p^2}, \dots, \tilde{B}_{n/p^k}$$

в подалгебре $\mathcal{M}(n, m)$ умножение дается формулой

$$\tilde{B}_{n/p^\alpha} \tilde{B}_{n/p^\beta} = \tilde{B}_{n/p^\alpha}, \quad \alpha \geq \beta.$$

Формула (4.9) сохраняется: пусть $d = n/(p_1^{\alpha_1} \dots p_s^{\alpha_s})$, тогда

$$\tilde{B}_d = \tilde{B}_{n/p_1^{\alpha_1}} \dots \tilde{B}_{n/p_s^{\alpha_s}}.$$

Введем в $\mathcal{M}(n)$ еще один базис $\{V_d\}$:

$$V_d = \sum_{c|d} \mu\left(\frac{d}{c}\right) \tilde{B}_c, \quad (4.11)$$

так что

$$\tilde{B}_c = \sum_{d|c} V_d. \quad (4.12)$$

ТЕОРЕМА 4.6. *Базис $\{V_d\}$ образован ортогональными идемпотентами:*

$$V_d^2 = V_d, \quad (4.13)$$

$$V_d V_c = 0, \quad c \neq d. \quad (4.14)$$

Он состоит из общих собственных векторов для операторов умножения на элементы из алгебры $\mathcal{M}(n)$. А именно, пусть F – произвольный элемент из $\mathcal{M}(n)$, разложим его по базису $\{V_c\}$:

$$F = \sum_{c|n} f(c) V_c,$$

коэффициенты $f(c)$ этого разложения являются собственными числами оператора умножения на F в $\mathcal{M}(n)$. В частности, для $\tilde{B}_c$ имеем

$$\tilde{B}_c V_d = \begin{cases} V_d, & d | c, \\ 0, & d \nmid c. \end{cases} \quad (4.15)$$

ДОКАЗАТЕЛЬСТВО. Докажем сначала (4.15). Пусть

$$d = \frac{n}{p_1^{\alpha_1} \dots p_s^{\alpha_s}}, \quad c = \frac{n}{p_1^{r_1} \dots p_s^{r_s}}. \quad (4.16)$$

Используя мультипликативность функции Мёбиуса, разложим (4.11) в произведение по примарным подалгебрам:

$$V_d = V_{n/p_1^{\alpha_1}}^{(1)} \dots V_{n/p_s^{\alpha_s}}^{(s)},$$

где

$$V_{n/p_i^{\alpha_i}}^{(i)} = \sum_{\beta \geq \alpha_i} \mu(p_i^{\beta - \alpha_i}) \tilde{B}_{n/p_i^\beta};$$

последняя формула означает, что

$$V_{n/p_i^{\alpha_i}}^{(i)} = \tilde{B}_{n/p_i^{\alpha_i}} - \tilde{B}_{n/p_i^{\alpha_i+1}}, \quad 0 \leq \alpha_i < k_i, \quad (4.17)$$

$$V_{n/p_i^{k_i}}^{(i)} = \tilde{B}_{n/p_i^{k_i}}. \quad (4.18)$$

Пусть сначала d делит c . Тогда $\alpha_i \geq r_i$ для всех $i = 1, \dots, s$. Следовательно, по (4.7) имеем

$$\tilde{B}_{n/p_i^{r_i}} V_{n/p_i^{\alpha_i}}^{(i)} = V_{n/p_i^{\alpha_i}}^{(i)},$$

так что $\tilde{B}_c V_d = V_d$.

Если же d не делит c , то хотя бы для одного i имеем $\alpha_i < r_i$; тогда по (4.7) для этого i получаем

$$\tilde{B}_{n/p_i^{r_i}} V_{n/p_i^{\alpha_i}}^{(i)} = \tilde{B}_{n/p_i^{r_i}} (\tilde{B}_{n/p_i^{\alpha_i}} - \tilde{B}_{n/p_i^{\alpha_i+1}}) = \tilde{B}_{n/p_i^{r_i}} - \tilde{B}_{n/p_i^{r_i}} = 0,$$

так что $\tilde{B}_c V_d = 0$.

Теперь докажем (4.13). По (4.11) имеем

$$V_d^2 = \sum_{c|d} \mu\left(\frac{d}{c}\right) V_d \tilde{B}_c.$$

По (4.15) здесь только одно слагаемое отлично от нуля – то, для которого $c = d$, оно равно $\mu(1) V_d = V_d$.

Наконец докажем (4.14). Пусть $d < c$. По (4.11) имеем

$$V_d V_c = \sum_{a|d} \mu\left(\frac{d}{a}\right) \tilde{B}_a V_c.$$

Так как a делит d , то $a < c$. Следовательно, c не делит a , так что по (4.15) $\tilde{B}_a V_c = 0$ и потому $V_d V_c = 0$.

Вернемся к базису $\{A_d\}$.

ТЕОРЕМА 4.7. *Элементы*

$$A_n, A_{n/p}, A_{n/p^2}, \dots, A_{n/p^k}, \quad (4.19)$$

где p – один из $p_1, \dots, p_s$, принадлежат примарной подалгебре $\mathcal{M}(n, t)$, $t = p^k$, и образуют в ней базис. Этот базис и базис (4.6) выражаются друг через друга следующим образом:

$$B_{n/p^\alpha} = \sum_{r \leq \alpha} A_{n/p^r}, \quad (4.20)$$

$$A_{n/p^\alpha} = B_{n/p^\alpha} - B_{n/p^{\alpha-1}}, \quad 0 < \alpha \leq k, \quad (4.21)$$

$$A_n = B_n. \quad (4.22)$$

Всякий элемент A_d разлагается в произведение элементов из примарных подалгебр:

$$A_{n/(p_1^{\alpha_1} \dots p_s^{\alpha_s})} = A_{n/p_1^{\alpha_1}} \dots A_{n/p_s^{\alpha_s}}. \quad (4.23)$$

ДОКАЗАТЕЛЬСТВО. Формулы (4.20)–(4.22) сразу следуют из (4.2), (4.3). Они показывают, что элементы (4.19) в самом деле образуют базис в $\mathcal{M}(n, m)$. Равенство (4.23) следует из (4.9) и мультипликативности функции Мёбиуса. В самом деле, пусть $d = n/(p_1^{\alpha_1} \dots p_s^{\alpha_s})$; тогда по (4.3), (4.9) и (4.21), (4.22) мы имеем (далее $\alpha_i \geq r_i$)

$$\begin{aligned} A_d &= \sum \mu(p_1^{\alpha_1 - r_1} \dots p_s^{\alpha_s - r_s}) B_{n/(p_1^{r_1} \dots p_s^{r_s})} \\ &= \sum \mu(p_1^{\alpha_1 - r_1}) \dots \mu(p_s^{\alpha_s - r_s}) B_{n/p_1^{r_1}} \dots B_{n/p_s^{r_s}} \\ &= \sum \mu(p_1^{\alpha_1 - r_1}) B_{n/p_1^{r_1}} \dots \sum \mu(p_s^{\alpha_s - r_s}) B_{n/p_s^{r_s}} = A_{n/p_1^{\alpha_1}} \dots A_{n/p_s^{\alpha_s}}. \end{aligned}$$

Теперь разложим по базису $\{A_f\}$ произведение $A_d A_c$ для произвольных d и c . Пусть d и c даются формулами (4.16). Их наибольший общий делитель есть

$$(d, c) = \frac{n}{p_1^{b_1} \dots p_s^{b_s}}, \quad b_i = \max\{\alpha_i, r_i\}. \quad (4.24)$$

Пусть I – множество индексов i из $\{1, 2, \dots, s\}$ таких, что $\alpha_i = r_i$. Представим (d, c) в виде

$$(d, c) = \frac{n}{wx}, \quad w = \prod_{i \in I} p_i^{b_i}, \quad x = \prod_{i \notin I} p_i^{b_i}. \quad (4.25)$$

Введем следующую функцию Q_N натурального переменного:

$$Q_N(y) = \sum_{u|y} \frac{\mu(u)}{\varphi_N(u)},$$

в частности, $Q_N(1) = 1$; эта функция мультипликативная.

Для $a = p_1^{u_1} \dots p_s^{u_s}$ обозначим через $\bar{a}$ число, полученное “освобождением от кратностей”: $\bar{a} = \prod p_j$, произведение берется по тем j , для которых $u_j \geq 1$.

Для числа a и его делителя b определим число

$$\xi(a, b) = \frac{\bar{a}}{a/b}.$$

ТЕОРЕМА 4.8. Для чисел d и c определим числа w и x , как указано выше (см. (4.24), (4.25)). Пусть $[d, c]$ – наименьшее общее кратное чисел d и c . Имеет место формула

$$A_d A_c = \varphi_N\left(\frac{n}{[d, c]}\right) \sum_{z|w} Q_N(\xi(w, z)) A_{n/(zx)}. \quad (4.26)$$

В частности, если I пусто, так что $w = 1$, то

$$A_d A_c = \varphi_N\left(\frac{n}{[d, c]}\right) A_{(d, c)}, \quad (4.27)$$

а если $d = c$, то $I = \{1, 2, \dots, s\}$, $w = n/d$, $x = 1$, так что

$$A_d^2 = \varphi_N\left(\frac{n}{d}\right) \sum_{d|v} Q_N\left(\xi\left(\frac{n}{d}, \frac{n}{v}\right)\right) A_v. \quad (4.28)$$

ДОКАЗАТЕЛЬСТВО. Возьмем примарную подалгебру $\mathcal{M}(n, m)$ и в ней два элемента A_{n/p^α} и A_{n/p^β} , $\alpha \geq \beta > 0$, и вычислим их произведение. Пусть сначала $\alpha > \beta$. Тогда по (4.21) и (4.7) имеем

$$\begin{aligned} A_{n/p^\alpha} A_{n/p^\beta} &= (B_{n/p^\alpha} - B_{n/p^{\alpha-1}})(B_{n/p^\beta} - B_{n/p^{\beta-1}}) \\ &= p^{\beta N} B_{n/p^\alpha} - p^{\beta N} B_{n/p^{\alpha-1}} - p^{(\beta-1)N} B_{n/p^\alpha} + p^{(\beta-1)N} B_{n/p^{\alpha-1}} \\ &= (p^{\beta N} - p^{(\beta-1)N})(B_{n/p^\alpha} - B_{n/p^{\alpha-1}}) = \varphi_N(p^\beta) A_{n/p^\alpha}. \end{aligned}$$

Таким образом, формула (4.27) справедлива для элементов из примарной подалгебры при $w = 1$, т.е. $d \neq c$ (при $\alpha = 0$ или $\beta = 0$ формула выполняется тривиальным образом, поскольку $A_n = E$).

По мультипликативности формула (4.27) справедлива для любых A_d и A_c таких, что $w = 1$.

Вернемся к $\mathcal{M}(n, m)$. Пусть теперь $\alpha = \beta$. Вычислим квадрат элемента A_{n/p^α} . По (4.21) и (4.7) имеем

$$A_{n/p^\alpha}^2 = (p^{\alpha N} - 2p^{(\alpha-1)N})B_{n/p^\alpha} + p^{(\alpha-1)N}B_{n/p^{\alpha-1}}.$$

Подставив сюда (4.20), мы получим

$$\begin{aligned} A_{n/p^\alpha}^2 &= (p^{\alpha N} - p^{(\alpha-1)N}) \sum_{r < \alpha} A_{n/p^r} + (p^{\alpha N} - 2p^{(\alpha-1)N}) A_{n/p^\alpha} \\ &= \varphi_N(p^\alpha) \left\{ \sum_{r < \alpha} A_{n/p^r} + \frac{1 - 2p^{-N}}{1 - p^{-N}} A_{n/p^\alpha} \right\}. \end{aligned} \quad (4.29)$$

Дробь здесь можно переписать в виде

$$1 - \frac{1}{p^N(1 - p^{-N})},$$

это в точности $Q_N(p)$. Число $\xi(n/d, n/v)$ из (4.28) для $d = n/p^\alpha$ и $v = n/p^r$, $r \leq \alpha$, равно

$$\xi(p^\alpha, p^r) = \frac{\overline{p^\alpha}}{p^{\alpha-r}} = \begin{cases} 1, & r < \alpha, \\ p, & r = \alpha. \end{cases}$$

Поэтому (4.29) есть

$$A_{n/p^\alpha}^2 = \varphi_N(p^\alpha) \sum_{r \leq \alpha} Q(\xi(p^\alpha, p^r)) A_{n/p^r},$$

что доказывает (4.28) для A_d из примарной подалгебры и по мультипликативности — для любых A_d .

Теперь докажем (4.26) для произвольных A_d и A_c . Разложим (d, c) , как указано в (4.25). Тогда

$$d = \frac{n}{w \cdot \tau}, \quad c = \frac{n}{w \cdot \theta},$$

где τ и θ разлагаются по множителям p_i , $i \notin I$:

$$\tau = \prod_{i \notin I} p_i^{\gamma_i}, \quad \theta = \prod_{i \notin I} p_i^{\delta_i}, \quad \gamma_i \neq \delta_i,$$

так что, в частности,

$$\left(\frac{n}{\tau}, \frac{n}{\theta}\right) = \frac{n}{x}, \quad \left[\frac{n}{\tau}, \frac{n}{\theta}\right] = \frac{n}{\tau, \theta}.$$

По (4.23) имеем

$$A_d = A_{n/w} A_{n/\tau}, \quad A_c = A_{n/w} A_{n/\theta},$$

так что

$$A_d A_c = A_{n/w}^2 A_{n/\tau} A_{n/\theta}. \quad (4.30)$$

К произведению двух последних множителей применим (4.27), получим

$$A_{n/\tau} A_{n/\theta} = \varphi_N \left(\frac{n}{[n/\tau, n/\theta]} \right) A_{(n/\tau, n/\theta)} = \varphi_N((\tau, \theta)) A_{n/x}, \quad (4.31)$$

а первый множитель в правой части (квадрат $A_{n/w}^2$) разложим по (4.28):

$$A_{n/w}^2 = \varphi_N(w) \sum_{z|w} Q_N(\xi(w, z)) A_{n/z}. \quad (4.32)$$

Теперь подставляем (4.31) и (4.32) в (4.30). Пара w и (τ, θ) , а также пара n/z и n/x не имеют общих простых делителей p_i , поэтому $A_{n/z} A_{n/x} = A_{n/(zx)}$ и

$$\varphi_N(w) \varphi_N((\tau, \theta)) = \varphi_N(w \cdot (\tau, \theta)) = \varphi_N \left(\frac{n}{[d, c]} \right).$$

Это и доказывает (4.26).

Наконец выразим базисы A_d и $\{V_c\}$ друг через друга:

$$A_d = \sum a(d, c) V_c, \quad (4.33)$$

$$V_c = \sum v(c, d) A_d. \quad (4.34)$$

Представим дробь c/d в виде несократимой дроби: $c/d = c'/d'$. В частности, если c делит d , то $c' = 1$. Такое представление мультипликативно. Это означает, что если c и d разложены на примарные множители: $c = c_1 \cdots c_s$, $d = d_1 \cdots d_s$, то $c' = c'_1, \dots, c'_s$.

ТЕОРЕМА 4.9. *Имеют место формулы*

$$a(d, c) = \frac{\mu(c')}{\varphi_N(c')} \varphi_N \left(\frac{n}{d} \right), \quad (4.35)$$

$$v(c, d) = \frac{\mu(c')}{\varphi_N(c')} \varphi_N \left(\frac{n}{c} \right) \cdot \left(\frac{n}{c} \right)^{-2N}. \quad (4.36)$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим примарную подалгебру $\mathcal{M}(n, m_i)$, $m_i = p_i^{k_i}$. Для краткости опустим индекс i и будем писать W_{n/p^r} вместо $V_{n/p^r}^{(i)}$. В этой

подалгебре имеют место разложения

$$A_{n/p^\alpha} = p^{\alpha N} \tilde{B}_{n/p^\alpha} - p^{(\alpha-1)N} \tilde{B}_{n/p^{\alpha-1}}, \quad (4.37)$$

$$B_{n/p^\alpha} = \sum_{r \leq \alpha} A_{n/p^r}, \quad (4.38)$$

$$\tilde{B}_{n/p^r} = \sum_{t \geq r} W_{n/p^t}, \quad (4.39)$$

$$W_{n/p^\alpha} = p^{-\alpha N} B_{n/p^\alpha} - p^{-(\alpha+1)N} B_{n/p^{\alpha+1}}, \quad (4.40)$$

в формулах (4.37) и (4.40) последние слагаемые отсутствуют при $\alpha = 0$ и $\alpha = k$ соответственно. Эти разложения вытекают из (4.21), (4.22), (4.10), (4.2), (4.12), (4.17), (4.18). Подставив (4.39) в (4.37), мы получим

$$A_{n/p^\alpha} = -p^{(\alpha-1)N} W_{n/p^{\alpha-1}} + \varphi_N(p^\alpha) \sum_{r \geq \alpha} W_{n/p^r}; \quad (4.41)$$

первое слагаемое в правой части отсутствует при $\alpha = 0$. С другой стороны, для $d = n/p^\alpha$ и $c = n/p^r$ мы имеем $c/d = p^{\alpha-r}$, так что $c' = 1$ для $r \geq \alpha$, $c' = p^{\alpha-r}$ для $r < \alpha$. Поэтому $\mu(c') = 1$ для $r \geq \alpha$, $\mu(c') = -1$ для $r = \alpha - 1$, $\mu(c') = 0$ для $r < \alpha - 1$. Следовательно, для $d = n/p^\alpha$ и $c = n/p^r$ коэффициент $a(d, c)$, задаваемый (4.35), совпадает с соответствующим коэффициентом в правой части (4.41). Это доказывает (4.33) с (4.35) для примарной подалгебры и по мультипликативности – для всей алгебры $\mathcal{M}(n)$.

Аналогично, подставив (4.38) в (4.40), мы получим

$$W_{n/p^\alpha} = -p^{-(\alpha+1)N} A_{n/p^{\alpha+1}} + p^{-\alpha N} (1 - p^{-N}) \sum_{r \leq \alpha} A_{n/p^r}; \quad (4.42)$$

первое слагаемое в правой части отсутствует при $\alpha = k$. С другой стороны, для $c = n/p^\alpha$ и $d = n/p^r$ мы имеем $c/d = p^{r-\alpha}$, так что $c' = 1$ для $r \leq \alpha$, $c' = p^{r-\alpha}$ для $r > \alpha$. Поэтому $\mu(c') = 1$ для $r \leq \alpha$, $\mu(c') = -1$ для $r = \alpha + 1$, $\mu(c') = 0$ для $r > \alpha + 1$. Следовательно, для $c = n/p^\alpha$ и $d = n/p^r$ коэффициент $v(c, d)$, задаваемый (4.36), совпадает с соответствующим коэффициентом в правой части (4.42). Это доказывает (4.34) с (4.36) для примарной подалгебры и по мультипликативности – для всей алгебры $\mathcal{M}(n)$.

§ 5. Преобразование Радона для $\mathbb{Z}_n^N$

ТЕОРЕМА 5.1. *Количество гиперплоскостей из H_0 (т.е. гиперплоскостей, проходящих через начало координат), проходящих через всякую из точек множества A_d , есть*

$$t(n, d) = \frac{\varphi_N(n)}{\varphi_1(n)} \frac{\varphi_{N-1}(n/d)}{\varphi_N(n/d)}. \quad (5.1)$$

ДОКАЗАТЕЛЬСТВО. Напомним, что группа G действует транзитивно на каждом множестве A_d и что $|A_d| = \varphi_N(n/d)$. Всякая гиперплоскость из H_0 задается уравнением $\langle a, x \rangle = 0$, $a \in A_1$, причем векторы a и ra , где r взаимно просто с n , задают одну и ту же гиперплоскость. Поэтому, во-первых, группа G действует

транзитивно на H_0 и, во-вторых, количество всех гиперплоскостей в H_0 равно $|A_1|/\varphi_1(n) = \varphi_N(n)/\varphi_1(n)$. С другой стороны, на каждой гиперплоскости из H_0 имеется $\varphi_{N-1}(n/d)$ точек из A_d (например, пересечение множества A_d с гиперплоскостью $x_N = 0$ есть множество A_d для пространства $\mathbb{Z}_n^{N-1}$, по теореме 4.1 количество точек в этом множестве есть $\varphi_{N-1}(n/d)$). Поэтому

$$\frac{\varphi_N(n)}{\varphi_1(n)} \varphi_{N-1}\left(\frac{n}{d}\right) = t(n, d) \varphi_N\left(\frac{n}{d}\right),$$

откуда получаем (5.1).

Функция $t(n, d)$, определенная в (5.1), удовлетворяет условию

$$t\left(n, \frac{n}{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}\right) = t\left(m_1, \frac{m_1}{p_1^{\alpha_1}}\right) \cdots t\left(m_s, \frac{m_s}{p_s^{\alpha_s}}\right). \quad (5.2)$$

Для $m = p^k$ мы имеем

$$t\left(m, \frac{m}{p^r}\right) = \begin{cases} p^{(N-1)(k-1)-(r-1)} \frac{p^{N-1} - 1}{p - 1}, & 0 < r \leq k, \\ p^{(N-1)(k-1)} \frac{p^N - 1}{p - 1}, & r = 0. \end{cases}$$

По теореме 5.1 элемент T из $\mathcal{M}(n)$ (см. § 2) есть

$$T = \sum_{d|n} t(n, d) A_d.$$

ТЕОРЕМА 5.2. *Элемент T из $\mathcal{M}(n)$ является “чистым тензором”, он разлагается в произведение элементов из примарных подалгебр:*

$$T = T(m_1) \cdots T(m_s), \quad T(m_i) \in \mathcal{M}(n, m_i),$$

где

$$T(m_i) = \sum_{\alpha=0}^{k_i} t\left(m_i, \frac{m_i}{p_i^\alpha}\right) A_{n/p_i^\alpha}.$$

Теорема следует из формул (5.2) и (4.23).

Теперь разложим элемент T по другим базисам:

$$T = \sum_{d|n} b(n, d) B_d, \quad (5.3)$$

$$T = \sum_{d|n} \tilde{b}(n, d) \tilde{B}_d, \quad (5.4)$$

$$T = \sum_{d|n} \lambda(n, d) V_d. \quad (5.5)$$

По (4.10) коэффициенты в (5.3) и (5.4) связаны соотношением

$$\tilde{b}(n, d) = \left(\frac{n}{d}\right)^N b(n, d). \quad (5.6)$$

ТЕОРЕМА 5.3. Коэффициенты разложений (5.3) и (5.5) выражаются следующими формулами:

$$b(n, d) = d^{N-1} \varphi_{N-1} \left(\frac{n}{d} \right) \frac{\varphi_1(d)}{\varphi_1(n)}, \quad (5.7)$$

$$\lambda(n, d) = n^{N-1} \frac{\varphi_N(n)}{\varphi_N(d)} \frac{\varphi_1(d)}{\varphi_1(n)}. \quad (5.8)$$

ДОКАЗАТЕЛЬСТВО. В силу (4.3) коэффициенты $b(n, d)$ выражаются через $t(n, d)$:

$$b(n, d) = \sum_{c|d} \mu \left(\frac{d}{c} \right) t(n, c).$$

Подставим сюда (5.1) и используем (3.7), где надо взять $R = N$, $L = 1$. Мы получим (5.7).

По (5.6) и (5.7) находим $\tilde{b}(n, d)$:

$$\tilde{b}(n, d) = n^N \frac{\varphi_{N-1}(n/d) \varphi_1(d)}{d \cdot \varphi_1(n)}. \quad (5.9)$$

В силу (4.12) коэффициенты $\lambda(n, d)$ выражаются через $\tilde{b}(n, d)$:

$$\lambda(n, d) = \sum_{d|c} \tilde{b}(n, c).$$

Подставим сюда (5.9) и используем (3.6), где снова надо взять $R = N$, $L = 1$. Мы получим (5.8).

ТЕОРЕМА 5.4. Элемент T имеет в алгебре $\mathcal{M}(n)$ обратный элемент T^{-1} . Его разложение по базису $\{B_d\}$ есть

$$T^{-1} = \sum_{d|n} y(n, d) B_d, \quad (5.10)$$

где

$$y(n, d) = n^{1-N} \frac{\varphi_N(d) \varphi_{1-N}(n/d)}{\varphi_N(n)}. \quad (5.11)$$

ДОКАЗАТЕЛЬСТВО. Числа $\lambda(n, d)$ (см. (5.8)) являются собственными числами оператора умножения на T в алгебре $\mathcal{M}(n)$. Мы видим, что они положительны. Следовательно, T имеет в алгебре $\mathcal{M}(n)$ обратный элемент

$$T^{-1} = \sum_{d|n} \lambda(n, d)^{-1} V_d.$$

Разложим T^{-1} по базису $\{\tilde{B}_d\}$:

$$T^{-1} = \sum_{d|n} \tilde{y}(n, d) \tilde{B}_d.$$

В силу (4.11) коэффициенты $\tilde{y}(n, d)$ выражаются через $\lambda(n, d)^{-1}$:

$$\tilde{y}(n, d) = \sum_{d|c} \mu\left(\frac{c}{d}\right) \lambda(n, c)^{-1}.$$

Подставим сюда вместо коэффициентов λ их выражения (5.8) и применим (3.7), где надо взять $R = 1$, $L = 1 - N$ и заменить c и d на n/c и n/d соответственно. Мы получим

$$\tilde{y}(n, d) = n \cdot d^{-N} \frac{\varphi_N(d) \varphi_{1-N}(n/d)}{\varphi_N(n)}.$$

Остается умножить это на $(n/d)^{-N}$, чтобы получить (5.11), поскольку $y(n, d) = (n/d)^{-N} \tilde{y}(n, d)$.

Разложение элемента T^{-1} по базису $\{A_c\}$ имеет более сложные коэффициенты. Ради полноты приведем их выражения.

ТЕОРЕМА 5.5. Пусть

$$T^{-1} = \sum \hat{t}(n, c) A_c.$$

Для $c = p_1^{r_1} \cdots p_s^{r_s}$ мы имеем

$$\hat{t}(n, c) = \frac{n^{1-2N} \varphi_{1-N}^2(n)}{\varphi_N(n) \varphi_{1-2N}(n)} \cdot x(n, c), \quad (5.12)$$

где

$$\begin{aligned} x(n, c) &= \prod x(m_i, p_i^{r_i}), \\ x(m, p^r) &= 1 - \left(\frac{p^{-N} - 1}{p^{N-1} - 1} \right)^\varepsilon p^{(2N-1)(r+1)}, \end{aligned} \quad (5.13)$$

$\varepsilon = 1$ при $r < k$, $\varepsilon = 2$ при $r = k$.

ДОКАЗАТЕЛЬСТВО. Из (5.10), (5.11) и (4.2) получаем

$$\hat{t}(n, c) = \frac{n^{1-N}}{\varphi_N(n)} t^*(n, c), \quad (5.14)$$

где

$$t^*(n, c) = \sum_{d|c} \varphi_N(d) \varphi_{1-N}\left(\frac{n}{d}\right).$$

Функция $t^*(n, c)$ распадается в произведение таких же функций для примарных подалгебр: пусть $c = p_1^{r_1} \cdots p_s^{r_s}$; тогда

$$t^*(n, c) = \prod_{i=1}^s t^*(p_i^{k_i}, p_i^{r_i}),$$

где

$$t^*(p^k, p^r) = \sum_{0 \leq \alpha \leq r} \varphi_N(p^\alpha) \varphi_{1-N}(p^{k-\alpha}). \quad (5.15)$$

По определению функций Эйлера (3.3), (3.4) мы имеем

$$\begin{aligned}\varphi_N(p^\alpha) &= p^{\alpha N}(1 - p^{-N}), & \alpha > 0, \\ \varphi_{1-N}(p^{k-\alpha}) &= p^{(k-\alpha)(1-N)}(1 - p^{N-1}), & \alpha < k,\end{aligned}$$

а также $\varphi_N(1) = \varphi_{1-N}(1) = 1$. Подставив это в (5.15), получим сумму, которая есть геометрическая прогрессия со знаменателем p^{2N-1} плюс еще один или два члена. Суммируя прогрессию, мы получаем

$$t^*(p^k, p^r) = \frac{(p^{N-1} - 1)^2 p^{k(1-N)}}{1 - p^{2N-1}} \cdot x(p^k, p^r),$$

где $x(p^k, p^r)$ дается формулой (5.13). Последнюю дробь можно записать в виде

$$\frac{p^{-kN} \varphi_{1-N}^2(p^k)}{\varphi_{1-2N}(p^k)}.$$

Вместе с множителем перед t^* в (5.14) она дает множитель перед x в (5.12).

Список литературы

- [1] М. И. Граев, Н. В. Павленко, “Преобразование Радона в пространстве $P^n(A)$, где A – конечное коммутативное кольцо с единицей”, *Докл. АН СССР*, **207**:2 (1972), 270–273; англ. пер.: М. И. Graev, N. V. Pavlenko, “The Radon transformation in the space $P^n(A)$ where A is a finite commutative ring with identity”, *Soviet Math. Dokl.*, **13**:4 (1972), 1493–1497.
- [2] М. Холл, *Комбинаторика*, Мир, М., 1970; пер. с англ.: М. Hall, *Combinatorial theory*, Blaisdell Publ., Waltham, MA–Toronto–London, 1967.

В. Ф. Молчанов (V. F. Molchanov)

Тамбовский государственный университет
им. Г. Р. Державина

E-mail: v.molchanov@bk.ru

Поступила в редакцию

29.12.2010 и 29.12.2011