Math-Net.Ru

Общероссийский математический портал

В. М. Бухштабер, А. М. Вершик, С. А. Евдокимов, И. Н. Пономаренко, Комбинаторные алгебры и многозначные инволютивные группы, *Функци. анализ и его прил.*, 1996, том 30, выпуск 3, 12–18

DOI: <https://doi.org/10.4213/faa531>

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: 3.95.254.165

26 апреля 2023 г., 13:48:25

УДК 517.986

Комбинаторные алгебры и многозначные инволютивные группы

© 1996. В. М. БУХШТАБЕР, А. М. ВЕРШИК,
С. А. ЕВДОКИМОВ, И. Н. ПОНОМАРЕНКО

§1. Основные определения

Назовем n -мультимножеством данного множества X неупорядоченный набор из n элементов $x_1, \dots, x_n \in X$. Совокупность всех n -мультимножеств есть n -я симметрическая степень $(X)^n$ множества X .

ОПРЕДЕЛЕНИЕ 1.1 (см. [2]). *Многозначная (n -значная) группа* — это тройка $\mathcal{X} = (X, \cdot, *)$, в которой X есть множество с заданными операциями умножения $\cdot$ и взятия обратного $*$; операция умножения каждой паре элементов x и y из X ставит в соответствие n -мультимножество $x \cdot y \in (X)^n$ с элементами $(x \cdot y)_1, \dots, (x \cdot y)_n$ из X , а операция $*$ переводит X в X . При этом выполняются следующие аксиомы:

(M1) (*аксиома единицы*) существует элемент $e \in X$, такой, что

$$\forall x \in X \quad (x \cdot e)_i = (e \cdot x)_i = x, \quad i = 1, \dots, n.$$

(M2) (*аксиома ассоциативности*) n^2 -мультимножества

$$\{((x \cdot y)_i \cdot z)_j\}_{i,j=1}^n, \quad \{(x \cdot (y \cdot z)_i)_j\}_{i,j=1}^n$$

совпадают для любых x, y и z из X .

(M3) (*аксиома обратного элемента*) e входит в n -мультимножества $x \cdot x^*$ и $x^* \cdot x$.

Многозначная группа называется *коммутативной*, если n -мультимножества $x \cdot y$ и $y \cdot x$ совпадают для любых x и y .

Детальный анализ аксиом n -значных групп и различные естественные их варианты содержатся в [2]. Обратим внимание, что здесь мы изучаем только алгебраические аспекты, т.е. в отличие от [2] не рассматриваем эффекты, связанные с топологией множества X . В дальнейшем мы сводим изучение многозначных групп к изучению их групповых алгебр.

Первые важные примеры n -значных групп возникают из следующей конструкции. Пусть G — некоторая группа и $A \subset \text{Aut}(G)$ — подгруппа порядка n . Тогда пространство $X = G/A$ орбит действия группы A на G имеет каноническую структуру n -значной группы с умножением, определяемым естественным образом умножением в G и проекцией $\pi: G \rightarrow X$ (см. [2]). Единицей в X является образ единицы группы G , а обратный элемент x^* к элементу x равен $\pi((\pi^{-1}(x))^{-1})$. Такие многозначные группы называются *косетными*. Более

общие примеры можно найти в [2]. Важные и новые примеры будут получены далее.

Для элементов x, y, z некоторой n -значной группы $\mathcal{X}$ обозначим через $m_{x,y}^z$ кратность, с которой z входит в мультимножество $x \cdot y$. Например, $m_{x,e}^x = n$.

ОПРЕДЕЛЕНИЕ 1.2. Многозначная группа $\mathcal{X} = (X, \cdot, *)$ называется *инволютивной*, если отображение $X \rightarrow X, x \mapsto x^*$, является инволюцией, удовлетворяющей условиям

- (I1) $\forall x \in X \quad x \cdot y \ni e \iff y = x^*$;
- (I2) $m(x) = m(x^*)$, где $m(x) = m_{x,x^*}^e$;
- (I3) $(x \cdot y)^* = y^* \cdot x^*$ для всех $x, y \in X$.

Заметим, что если инволюция $*$ удовлетворяет условию (I1), то она определена однозначно. Примером многозначной инволютивной группы является любая косетная многозначная группа. В то же время (см., в частности, [2]), легко привести примеры неинволютивных n -значных групп.

Групповой алгеброй $A(\mathcal{X})$ многозначной инволютивной группы назовем алгебру конечных формальных сумм элементов из X с умножением и инволюцией, продолженными по линейности (см. (2), (3) ниже). Ассоциативность и другие необходимые свойства алгебры $A(\mathcal{X})$ следуют из аксиом многозначных групп; при этом единица алгебры $A(\mathcal{X})$ совпадает с e , а n -мультимножеству $x_1, \dots, x_n$ отвечает элемент $\frac{1}{n} \sum_{i=1}^n x_i$ из $A(\mathcal{X})$.

Биекция $f: X \mapsto X'$ называется *изоморфизмом* n -значной группы $\mathcal{X} = (X, \cdot, *)$ на n' -значную группу $\mathcal{X}' = (X', \cdot, *)$, если

$$\frac{m_{x,y}^z}{n} = \frac{m_{x',y'}^{z'}}{n'}, \quad x, y, z \in X,$$

где $x' = f(x)$, $y' = f(y)$, $z' = f(z)$. Ясно, что в этом случае $f(e_X) = e_{X'}$ и $f(x^*) = f(x)^*$, $x \in X$. Легко видеть также, что f является изоморфизмом тогда и только тогда, когда отображение $A(\mathcal{X}) \rightarrow A(\mathcal{X}')$, задаваемое на базисе соответствием $x \mapsto f(x)$, является изоморфизмом алгебр.

Фактически ниже дается прямое описание групповых алгебр инволютивных многозначных групп, которое может быть использовано в качестве их определения. Этот класс алгебр уже встречался в алгебраической комбинаторике и теории двойственности алгебр.

Пусть A — ассоциативная алгебра над $\mathbf{C}$ с единицей 1 , полулинейным антиавтоморфизмом $*$ и выделенным линейным базисом $\mathcal{R}$. Для $r, s \in \mathcal{R}$ положим $r \cdot s = \sum_{t \in \mathcal{R}} c_{r,s}^t \cdot t$. Следующее понятие является видоизменением одного из объектов алгебраической комбинаторики.

ОПРЕДЕЛЕНИЕ 1.3. Пара $(A, \mathcal{R})$ называется *C-алгеброй*, если выполнены следующие условия:

- (C1) $1 \in \mathcal{R}$ и $\mathcal{R}^* = \mathcal{R}$;
- (C2) структурные константы $c_{r,s}^t$ алгебры A относительно базиса $\mathcal{R}$ вещественны;
- (C3) для всех $r, s \in \mathcal{R}$ имеет место равенство $c_{r,s}^1 = d(r)\delta_{r^*,s}$, где $d(r) > 0$ и δ — символ Кронекера;
- (C4) линейный функционал на A , задаваемый отображением $r \mapsto d(r)$, $r \in \mathcal{R}$, является одномерным $*$ -представлением алгебры A .

ЗАМЕЧАНИЕ 1.4. Если к условиям (C1)–(C4) добавить условие коммутативности и конечномерности алгебры A , то получится определение C -алгебры, или алгебры характеров, из [1]. Таким образом, по сравнению с [1] мы снимаем условие коммутативности и конечномерности.

ЗАМЕЧАНИЕ 1.5. Из условий (C4) и (C2) следует, что $d(r) = d(r^*)$ для всех $r \in \mathcal{R}$.

Изоморфизм $f: A \rightarrow B$ $*$ -алгебр с единицей называется изоморфизмом C -алгебры $(A, \mathcal{R})$ на C -алгебру $(B, \mathcal{S})$, если $f(\mathcal{R}) = \mathcal{S}$.

Для рационального числа a обозначим через $D(a)$ знаменатель (положительный) представления числа a в виде несократимой дроби.

ОПРЕДЕЛЕНИЕ 1.6. C -алгебра $(A, \mathcal{R})$ называется *комбинаторной алгеброй*, если все структурные константы $c_{r,s}^t$ алгебры A относительно базиса $\mathcal{R}$ суть неотрицательные рациональные числа и

$$D(c_{r,s}^t/d(r)) \leq D_0, \quad (1)$$

где D_0 не зависит от индексов r, s, t .

Заметим, что в конечномерном случае условие (1) является излишним. Многообразные примеры таких комбинаторных алгебр, возникающих из схем отношений, в том числе некоммутативных, можно найти в [1].

ЗАМЕЧАНИЕ 1.7. В алгебре с выделенным линейным базисом можно задать коммутативное умножение: покоординатное умножение на базисе и инволюцию — комплексное сопряжение координат; так обычно и делается в алгебраической комбинаторике и теории C -алгебр; в результате получается биалгебра, т. е. пространство с двумя умножениями, одно из которых коммутативно. Современный и более инвариантный подход, который уже переносится на произвольные алгебры, состоит в том, что с помощью базиса вводится не умножение, а кокоммутативное коумножение (диагональ). Коумножение позволяет избежать использования базиса и тем самым аксиоматизировать получающуюся структуру, которая включает умножение–коумножение, инволюцию–коинволюцию, единицу–коединицу. В случае многозначных групп или комбинаторных алгебр получаются алгебры, обобщающие понятие алгебр Хопфа с инволюцией: в алгебрах приведенного выше типа коумножение уже будет, вообще говоря, не кольцевым гомоморфизмом, как это требуется в аксиоматике алгебр Хопфа, а лишь положительным (в смысле инволюции) отображением $A \mapsto A \otimes A$. Аксиоматика алгебр с положительным коумножением была дана в несколько других терминах в работе [3] и изучена также в статье [4]. Подробнее эти связи будут рассмотрены в другой работе. Эта аксиоматика открывает возможность рассматривать и некокоммутативный случай — квантовые комбинаторные алгебры и квантовые многозначные группы. Как показано в [2], существуют универсальные формулы, связывающие умножение и коумножение в таких алгебрах; их аксиоматизация привела к понятию n -алгебр Хопфа, с точки зрения которого обычные алгебры Хопфа это 1-алгебры Хопфа.

§2. Конструкции и результаты

Приведем явный изоморфизм групповых алгебр многозначных инволютивных групп и соответствующих комбинаторных алгебр.

(а) Пусть $\mathcal{X} = (X, \cdot, *)$ есть n -значная инволютивная группа и $A = A(\mathcal{X})$ — ее групповая алгебра над $\mathbf{C}$. Формулы умножения и инволюции в $A(\mathcal{X})$ выглядят следующим образом:

$$x \cdot y = \frac{1}{n} \sum_{z \in X} m_{x,y}^z \cdot z, \quad x, y \in X, \quad (2)$$

$$\left(\sum_{x \in X} \alpha_x \cdot x \right)^* = \sum_{x \in X} \overline{\alpha_x} \cdot x^*. \quad (3)$$

Зафиксируем подмножество элементов из $A(\mathcal{X})$

$$\mathcal{R} = \mathcal{R}(\mathcal{X}) = \left\{ \frac{n}{m(x)} \cdot x \right\}_{x \in X}. \quad (4)$$

Очевидно, что $\mathcal{R}$ есть линейный базис в $A(\mathcal{X})$. Будем рассматривать пару $\mathcal{A}(\mathcal{X}) = (A(\mathcal{X}), \mathcal{R})$ как алгебру с базисом. Фактически мы заменили образующие x в алгебре $A(\mathcal{X})$ на $(n/m(x)) \cdot x$.

ТЕОРЕМА 2.1. *Алгебра с базисом $\mathcal{A}(\mathcal{X})$ есть комбинаторная алгебра.*

ДОКАЗАТЕЛЬСТВО. Свойство (C1) следует из построения групповой алгебры $A(\mathcal{X})$, условия (I2) и равенства $m(e) = n$. Из определения $\mathcal{R}(\mathcal{X})$ и формулы (2) имеем

$$c_{r,s}^t = \frac{m(z)}{m(x)m(y)} m_{x,y}^z, \quad r = \frac{n}{m(x)} \cdot x, \quad s = \frac{n}{m(y)} \cdot y, \quad t = \frac{n}{m(z)} \cdot z. \quad (5)$$

Из (I1) следует, что $m_{x,y}^e = m(x) \delta_{x^*,y}$. Таким образом, при $t = e$ из (5) и (I2) получаем

$$c_{r,s}^e = \frac{m(e)}{m(x)m(y)} m_{x,y}^e = \frac{n}{m(y)} \delta_{x^*,y} = \frac{n}{m(x)} \delta_{x^*,y} = d(r) \delta_{r^*,s},$$

где $d(r) = n/m(x)$, что доказывает (C3).

Поскольку $\sum_{z \in X} m_{x,y}^z = n$ для всех $x, y \in X$, линейный функционал на алгебре A , задаваемый отображением $x \mapsto 1$, $x \in X$, является ее одномерным характером. Значение этого характера на $r = (n/m(x)) \cdot x$ из $\mathcal{R}$ равно $n/m(x) = d(r)$. В силу (I2) получаем $d(r) = d(r^*)$, откуда следует (C4). Наконец, используя (5), заключаем, что $\mathcal{A}(\mathcal{X})$ является комбинаторной алгеброй. $\square$

(б) Пусть теперь $\mathcal{A} = (A, \mathcal{R})$ есть некоторая комбинаторная алгебра. Положим

$$X = X(\mathcal{A}) = \{r/d(r)\}_{r \in \mathcal{R}}, \quad (6)$$

и пусть

$$n = \text{H. O. K.}(D(c_{r,s}^t/d(r)))_{r,s,t \in \mathcal{R}}, \quad (7)$$

где $D(a)$ определено выше (из условия (1) следует, что $n < \infty$). Для $x, y, z \in X$ положим

$$m_{x,y}^z = n \cdot \frac{d(t) c_{r,s}^t}{d(r) d(s)}, \quad (8)$$

где $x = r/d(r)$, $y = s/d(s)$, $z = t/d(t)$. Используя ассоциативность умножения в A и вычисляя значение характера $d(r \cdot s \cdot t)$ двумя способами, получаем формулу

$$d(t) c_{r,s}^{t*} = d(r) c_{s,t}^{r*}.$$

Отсюда легко следует, что $m_{x,y}^z$ — неотрицательное целое число для всех $x, y, z \in X$. Обозначим через $x \cdot y$ мультимножество, в котором каждый элемент $z \in X$ содержится с кратностью $m_{x,y}^z$. Применяя характер из (С4) к равенству $r \cdot s = \sum_{t \in \mathcal{R}} c_{r,s}^t \cdot t$, получаем, что $d(r)d(s) = \sum_{t \in \mathcal{R}} c_{r,s}^t d(t)$, откуда следует, что $\sum_{z \in X} m_{x,y}^z = n$ для любых $x, y \in X$.

Определим инволюцию $*$ на X , полагая $(r/d(r))^* = r^*/d(r^*)$, $r \in \mathcal{R}$. Положим $\mathcal{X}(\mathcal{A}) = (X, \cdot, *)$.

ТЕОРЕМА 2.2. *Тройка $\mathcal{X}(\mathcal{A})$ есть n -значная инволютивная группа.*

ДОКАЗАТЕЛЬСТВО. Легко видеть (см. (8)), что отображение алгебры $A(\mathcal{X})$ в алгебру A , задаваемое для $x = r/d(r)$ соответствием $x \mapsto r/d(r)$, является $*$ -изоморфизмом алгебр, откуда следует ассоциативность алгебры $A(\mathcal{X})$ и наличие в ней единицы 1_A . Поэтому умножение $X \times X \rightarrow (X)^n$ ассоциативно, 1_A является единицей в X и для инволюции $*$ на X выполнено условие (I3). Для $x = r/d(r)$, $y = s/d(s)$ из X имеем, используя (8) и (С3),

$$m_{x,y}^e = n \cdot \frac{d(e) c_{r,s}^e}{d(r)d(s)} = \frac{nd(e)}{d(r)d(s)} \cdot d(r) \delta_{r^*,s} = \frac{n}{d(s)} \delta_{x^*,y},$$

откуда следует (I1) и равенство $m(x) = n/d(r^*)$. Наконец, из равенства $d(r) = d(r^*)$ (см. замечание 1.5) следует (I2). $\square$

ТЕОРЕМА 2.3. *Отображения*

$$\mathcal{X} \mapsto \mathcal{A}(\mathcal{X}), \quad \mathcal{A} \mapsto \mathcal{X}(\mathcal{A})$$

задают эквивалентность между категориями многозначных инволютивных групп и комбинаторных алгебр.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathcal{A} = (A, \mathcal{R})$ — комбинаторная алгебра. Прямым вычислением легко проверить, что соответствие $r \mapsto (n/m(x)) \cdot x$, $r \in \mathcal{R}$, где $x = r/d(r)$ и число n определено в (7), является изоморфизмом между комбинаторными алгебрами $\mathcal{A}$ и $\mathcal{A}(\mathcal{X}(\mathcal{A}))$. Обратно, пусть $\mathcal{X} = (X, \cdot, *)$ является n -значной инволютивной группой. Тогда соответствие $x \mapsto r/d(r)$, $x \in X$, где $r = (n/m(x)) \cdot x$, является изоморфизмом алгебры $A(\mathcal{X})$ на алгебру $A(\mathcal{Y})$, где $\mathcal{Y} = \mathcal{X}(\mathcal{A}(\mathcal{X}))$. Отсюда следует, что многозначные инволютивные группы $\mathcal{X}$ и $\mathcal{Y}$ изоморфны. $\square$

§3. Примеры

Групповая алгебра косетной многозначной группы (см. выше) есть подалгебра групповой алгебры исходной группы, порожденная элементами, совпадающими с суммами точек орбит действия группы автоморфизмов. Более общий пример группового происхождения — S-кольца, или кольца Шура (см. [5]), — получится, если разбиение на орбиты группы автоморфизмов в приведенном выше определении косетной группы заменить на произвольное разбиение, обладающее тем

же свойством: постоянные на блоках разбиения элементы групповой алгебры образуют ее инволютивную подалгебру. (В [3] и [4] такие разбиения были названы устойчивыми.) Однако имеется много примеров комбинаторных алгебр, не являющихся S-кольцами. Некоторые из них изучались в алгебраической комбинаторике в связи, например, с теорией дистанционно-регулярных графов. Из наших теорем вытекает, что эти примеры — один из них приводится ниже — дают примеры многозначных групп, не являющихся косетными и не имеющих групповой природы.

Рассмотрим следующее бесконечное семейство алгебр, задающих многозначные группы. Пусть $m = 4k + 3$, $k \geq 1$. Обозначим через $\mathcal{A}_m$ комбинаторную алгебру с базисом $\{1, r, s\}$, умножением

$$r^2 = k \cdot r + (k+1) \cdot s, \quad s^2 = (k+1) \cdot r + k \cdot s, \quad rs = sr = (2k+1) \cdot 1 + k \cdot r + k \cdot s$$

и инволюцией

$$r^* = s, \quad s^* = r.$$

Легко видеть в силу (7), что $\mathcal{X}(\mathcal{A}_m)$ является $(2k+1)$ -значной инволютивной группой на трехэлементном множестве $\{1, a, b\}$, в которой

$$\begin{aligned} a \cdot a &= \underbrace{\{a, \dots, a\}}_{k+1} \underbrace{\{b, \dots, b\}}_k, & b \cdot b &= \underbrace{\{a, \dots, a\}}_k \underbrace{\{b, \dots, b\}}_{k+1}, \\ a \cdot b &= b \cdot a = \{1, \underbrace{a, \dots, a}_k, \underbrace{b, \dots, b}_k\} \end{aligned}$$

и $a^* = b$, $b^* = a$.

В случае когда m является степенью простого числа вида $4k+3$, $k \geq 1$, комбинаторная алгебра $\mathcal{A}_m$ изоморфна алгебре Боуза–Меснера турнира Пэли над $\mathbf{GF}(m)$ (см. [1]) и, следовательно, $\mathcal{A}_m \cong \mathcal{A}(G/A)$, где G — аддитивная группа поля $\mathbf{GF}(m)$, а A — подгруппа индекса 2 его мультипликативной группы, действующая на G умножениями. В этом случае многозначная группа является косетной. (В общем случае вопрос о существовании для каждого m вида $4k+3$, $k \geq 1$, схемы отношений с алгеброй Боуза–Меснера, изоморфной алгебре $\mathcal{A}_m$, является открытым.)

ПРЕДЛОЖЕНИЕ 3.1. *Если $m = p \cdot q$, где p, q — различные нечетные простые числа, причем $pq \equiv 3 \pmod{4}$, то $\mathcal{X}(\mathcal{A}_m)$ не является косетной многозначной группой.*

ДОКАЗАТЕЛЬСТВО. Предположим противное. Пусть $\mathcal{X}(\mathcal{A}_m) \cong G/A$ для некоторой группы G и конечной группы $A \subset \text{Aut}(G)$ ее автоморфизмов. Тогда $\mathcal{A}_m \cong \mathcal{A}(G/A)$, откуда следует, что $|G| = d(1) + d(r) + d(s) = m$ и действие A на G имеет три орбиты порядков $1, 2k+1, 2k+1$. По теореме Силова силовская q -подгруппа группы G при $q > p$ является нормальной в G , а значит, и характеристической. Поэтому $q-1 = 2k+1$, что противоречит нечетности q . $\square$

ЗАМЕЧАНИЕ 3.2. В условиях предложения 3.1 комбинаторная алгебра $\mathcal{A}_m$ не является S-кольцом.

В следующих работах будет изучен специальный класс многозначных инволютивных групп и комбинаторных алгебр, обладающих свойством положительной

двойственности, введенной в [3]. Он охватывает комбинаторные алгебры, возникающие из схем отношений (см. [1]), и некоторые другие алгебры, в частности, выделяет важный подкласс многозначных групп, охватывающий косетные группы.

ЛИТЕРАТУРА

1. *Баннаи Э., Ито Т.* Алгебраическая комбинаторика I. Схемы отношений. Мир, М., 1987.
2. *Buchshtaber V. M., Rees E. G.* Multivalued groups, their representation and Hopf algebras. Preprint of Edinburg Univ. (1995).
3. *Вершик А. М.* Геометрическая теория состояний, граница фон Неймана, двойственность C^* -алгебр. Записки научн. сем. ЛОМИ, **29**, 147–154 (1972).
4. *Керов С. В.* Двойственность конечномерных C^* -алгебр. Вестник ЛГУ, сер. матем., №7, 23–29 (1974).
5. *Wielandt H.* Finite permutation groups. Academic Press, New York–London, 1964.

Математический институт
им. В. А. Стеклова РАН
Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН

Поступило в редакцию
25 мая 1996 г.