

n -значные группы, суммы Кронекера и матрицы Вендта

В.М.Бухштабер, М.И.Корнев

Математический институт им. В.А. Стеклова РАН
Математический центр мирового уровня МИАН
МГУ им. М.В.Ломоносова, мехмат.

Семинар С.П. Новикова
“Геометрия, топология и математическая физика”
МИАН–МГУ, Москва, 20 мая 2025

В различных областях исследований встречается естественное умножение на пространстве, скажем X , при котором произведением пары точек является подмножество в X .

Литература по многозначным группам и их приложениям велика и включает статьи начиная с 19 века, в основном, в контексте понятия гипергруппы.

В 1971 г. С.П. Новиков и автор ввели конструкцию, подсказанную теорией характеристических классов векторных расслоений, в которой произведение каждой пары элементов есть **n -мультимножество**, т.е. неупорядоченное множество из **n точек**, возможно с повторениями.

Эта конструкция привела к понятию **n -значной группы**.

Автор дал аксиоматическое определение n -значных формальных групп (n -ф групп) и развил их теорию в цикле работ.

Теорема (В.М. Бухштабер, 1976)

2-ф группа в комплексных кобордизмах является универсальной в классе 2-ф групп над кольцами без кручения при условии $\text{inv}(x) = x$.

Этот результат привел к решению задач алгебраической топологии и стимулировал развитие алгебраической теории n -значных групп.

В настоящее время рядом авторов получены результаты по теории n -значных групп (формальных, конечных, дискретных, топологических, алгебраических, алгебро-геометрических) с приложениями в различных областях математики и математической физики.

Симметрические степени пространства.

Для пространства X обозначим через $(X)^n$ его n -кратную симметрическую степень, т.е. $(X)^n = X^n / \Sigma_n$, где симметрическая группа Σ_n действует перестановкой сомножителей.

Точку в $(X)^n$ будем рассматривать как подмножество в X , состоящее из n точек (возможно с повторениями), т.е. как n -мультимножество (далее, n -множество).

Пример. Пространства $(\mathbb{C})^n = \mathbb{C}^n / \Sigma_n$ и $\mathbb{C}^n$ можно отождествить при помощи отображения

$$\mathcal{S} : \mathbb{C}^n \rightarrow \mathbb{C}^n : (z_1, z_2, \dots, z_n) \rightarrow e_r(z_1, z_2, \dots, z_n), \quad 1 \leq r \leq n,$$

где e_r — r -тый элементарный симметрический полином.

Проективизация отображения $\mathcal{S}$ индуцирует гомеоморфизм $(\mathbb{CP}^1)^n \rightarrow \mathbb{CP}^n$.

n -значные группы.

n -значное умножение на X задаётся отображением

$$\mu : X \times X \rightarrow (X)^n : \mu(x, y) = x * y = [z_1, \dots, z_n], \quad z_k = (x * y)_k.$$

Ассоциативность. n^2 -множества

$$\begin{aligned} &[x * (y * z)_1, x * (y * z)_2, \dots, x * (y * z)_n], \\ &[(x * y)_1 * z, (x * y)_2 * z, \dots, (x * y)_n * z] \end{aligned}$$

совпадают для всех $x, y, z \in X$.

Единица. Точка $e \in X$, такая, что $e * x = x * e = [x, x, \dots, x]$ для всех $x \in X$.

Обратный элемент. Отображение $\text{inv} : X \rightarrow X$, такое, что

$$e \in \text{inv}(x) * x \quad \text{and} \quad e \in x * \text{inv}(x) \quad \text{для всех } x \in X.$$

Коммутативность. n -множества $x * y$ и $y * x$ совпадают для всех $x, y \in X$.

Отображение μ определяет структуру n -значной группы на X , если оно ассоциативно и существуют e и inv .

Структура 2-значной группы на $\mathbb{Z}_+$.

Рассмотрим полугруппу по сложению неотрицательных целых чисел $\mathbb{Z}_+$.
Введем 2-значное коммутативное сложение на $\mathbb{Z}_+$

$$\mu: \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow (\mathbb{Z}_+)^2 : x * y = [x + y, |x - y|].$$

Единица: $e = 0$.

Обратный элемент: $\text{inv}(x) = x$.

Ассоциативность: 4-множества из $\mathbb{Z}_+$

$$[x + y + z, |x - y - z|, x + |y - z|, |x - |y - z||]$$

и

$$[x + y + z, |x + y - z|, |x - y| + z, ||x - y| - z|]$$

совпадают для любых $x, y, z \in \mathbb{Z}_+$.

Классификационная теорема

Двузначная группа на множестве X называется **инволютивной**, если мультимножество $x * y$ содержит единицу e тогда и только тогда, когда $x = y$.

Теорема (В.М.Бухштабер, А.П.Веселов, А.А.Гайфуллин, 2022)

- 1) Определены три серии конечно порождённых инволютивных коммутативных двузначных групп: основная, унипотентная и специальная.
- 2) Любая конечно порождённая инволютивная коммутативная двузначная группа изоморфна двузначной группе, принадлежащей одной из этих серий.

Теорема (А.А. Гайфуллин, 2024)

Всякая инволютивная двузначная группа коммутативна.

Алгебраические n -значные группы

Определение

Алгебраической n -значной группой называется алгебраическое многообразие X с n -значным умножением, которое определено на некотором плотном подмножестве $Y \subset X \times X$ в топологии Зарисского и удовлетворяет аксиомам n -значных групп.

Теория алгебраических n -значных групп и её связь с теорией интегрируемых динамических систем дискретного времени была развита в работах В.М.Бухштабера и А.П.Веселова.

Положим

$$P(z; x, y) = \sum_{k=0}^n F_k(x, y) z^{n-k}, \quad (1)$$

где $F_k(x, y) \in \mathbb{C}[x, y]$ и

$$F_0(0, 0) = 1. \quad (2)$$

Тогда определена операция $*$, которая сопоставляет элементам x и y на множестве комплексных чисел $\mathbb{C}$ мультимножество $x * y$ корней полинома (1) от переменной z .

Алгебраические n -значные группы

Из аксиомы нейтрального элемента $x = 0$ следует равенство

$$P(z; 0, y) = F_0(0, y)(z - y)^n. \quad (3)$$

Аксиома обратного элемента говорит о существовании алгебраического отображения $\text{inv} : \mathbb{C} \rightarrow \mathbb{C}$, такого, что для каждого $x \in \mathbb{C}$

$$F_n(x, \text{inv}(x)) = F_n(\text{inv}(x), x) = 0. \quad (4)$$

Обозначим через $z_j = z_j(x, y)$, $j = 1, \dots, n$, корни полинома P . Тогда условие ассоциативности записывается в виде тождественного равенства двух полиномов от переменной t

$$\prod_{i,j=1}^n (t - z_i(z_j(x, y), z)) = \prod_{i,j=1}^n (t - z_i(x, z_j(y, z))). \quad (5)$$

Уравнение ассоциативности

Положим $R_k(x, y) = \frac{F_k(x, y)}{F_0(x, y)}$.

Заметим, что

$$\prod_{i,j=1}^n (t - z_i(z_j(x, y), z)) = \prod_{j=1}^n \left(t^n + \sum_{k=1}^n R_k(z_j(x, y), z) t^{n-k} \right).$$

Таким образом, коэффициенты полиномов от t в уравнении ассоциативности (5) являются рациональными функциями от переменных x , y и z .

Определение

Назовем n -алгебраической n -значной группой на $\mathbb{C}$ алгебраическую n -значную группу с умножением

$$\begin{aligned} * : (\mathbb{C} \times \mathbb{C}) \setminus \{(x, y) \mid F_0(x, y) = 0\} &\longrightarrow \text{Sym}^n(\mathbb{C}), \\ (x, y) &\longmapsto [z_1, \dots, z_n] \end{aligned}$$

где z_j – корни полинома (1), такого, что каждая из переменных x и y входит в него в степени не выше n , и этот полином удовлетворяет условиям (2), (3), (4) и (5).

Соответствующую группу будем обозначать через $\mathbb{G}(P)$.

n -алгебраические n -значные группы

Из условия $F_0(0,0) = 1$ следует, что n -алгебраическая n -значная группа на $\mathbb{C}$ является **формальной n -значной группой** на $\mathbb{C}$ т.к. умножение в ней определено в окрестности $0 \in \mathbb{C}$.

Она определена на всем $\mathbb{C}$ тогда и только тогда, когда $F_0(x,y) \equiv 1$.

Пример

Пусть $P(z; x, y) = (1 + \alpha xy)z - x - y$, где $\alpha \in \mathbb{C}$.

Тогда 1-алгебраическая 1-значная коммутативная группа на $\mathbb{C}$ изоморфна алгебраической 1-значной группе матриц вида

$$\begin{pmatrix} 1 & x \\ \alpha x & 1 \end{pmatrix}$$

с точностью до умножения на ненулевые комплексные числа, поскольку имеет место равенство:

$$\begin{pmatrix} 1 & x \\ \alpha x & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ \alpha y & 1 \end{pmatrix} = (1 + \alpha xy) \begin{pmatrix} 1 & \frac{x+y}{1+\alpha xy} \\ \alpha \frac{x+y}{1+\alpha xy} & 1 \end{pmatrix}.$$

Симметрические n -алгебраические n -значные группы

Определение

n -алгебраическая n -значная группа называется **симметрической**, если полином $P(z; (-1)^n x, (-1)^n y)$ является симметрическим по x, y, z .

Теорема (В.М. Бухштабер, М.И. Корнев, 2025)

Универсальная симметрическая 2-алгебраическая 2-значная группа $\mathbb{G}(P)$ на $\mathbb{C}$ определена над кольцом коэффициентов

$$\mathbb{C}[k_2, k_4, k_6, k_8]/(4k_8 - k_4^2 + k_6 k_2) \cong \mathbb{C}[k_2, k_4, k_6],$$

т. е. универсальное семейство многочленов P_2 имеет вид:

$$P_2(z; x, y) = e_1^2 - 4e_2 + 2k_2 e_3 + (k_4^2 - k_6 k_2) e_3^2 + 2k_4 e a_1 e_3 + 2k_6 e_2 e_3.$$

Доказательство теоремы получено непосредственно из аксиом при помощи **системы компьютерной алгебры** Wolfram Mathematica.

Впервые этот результат был получен В.М.Бухштабером и А.П.Веселовым как следствие классификации двузначных формальных групп.

Симметрические n -алгебраические n -значные группы

Теорема (В.М. Бухштабер, М.И. Корнев, 2025)

Существует два класса симметрических 3-алгебраических 3-значных групп:

- 1 $P_3(z; -x, -y) = e_1^3 - 27e_3$. В этом случае мы получаем 3-значную группу $\mathbb{G}_3$.
- 2 $P_3(z; -x, -y) = (e_1 + \frac{\ell_4}{3}e_3)^3$. В этом случае соответствующая 3-значная группа получается диагональной конструкцией

$$G \times G \xrightarrow{\mu} G \xrightarrow{\text{Sym}^3 \circ \text{diag}} \text{Sym}^3(G)$$

из 1-значной алгебраической группы G , построенной по многочлену

$$P_1(z; -x, -y) = (1 + \frac{\ell_4}{3}xy)z + x + y = e_1 + \frac{\ell_4}{3}e_3.$$

Доказательство этого [нового результата](#) получено непосредственно из аксиом при помощи [системы компьютерной алгебры](#) Wolfram Mathematica.

n -значные группы $\mathbb{G}_n$ на $\mathbb{C}$.

Пусть $\varepsilon = \exp \frac{2\pi i}{n}$. Введем n -значное сложение

$$\mu: \mathbb{C} \times \mathbb{C} \rightarrow (\mathbb{C})^n : x * y = [z_1, \dots, z_n], \quad z_k = (\sqrt[n]{x} + \varepsilon^k \sqrt[n]{y})^n.$$

Единица: $e = 0$. Обратный элемент: $\text{inv}(x) = (-1)^n x$.

Получаем коммутативные алгебраические n -значные группы $\mathbb{G}_n$ с законом $p_n(z; x, y) = 0$, где

$$p_n(z; x, y) = (z - z_1) \cdots (z - z_k)$$

полиномы с целыми коэффициентами. Первые полиномы:

$$p_1 = z - x - y,$$

$$p_2 = (z + x + y)^2 - 4(xy + yz + zx),$$

$$p_3 = (z - x - y)^3 - 27xyz,$$

$$p_4 = ((z + y + x)^2 - 4(xy + yz + zx))^2 - 2^7(z + y + x)xyz.$$

Полином $p_n(z; (-1)^n x, (-1)^n y)$ является **симметрическим** по x, y, z и **однородным**.

Полиномы $P_n(e_1, e_2, e_3)$ и простые числа

Положим $P_n(e_1, e_2, e_3) = p_n(z; (-1)^n x, (-1)^n y)$, где e_1, e_2, e_3 – элементарные симметрические полиномы.

$$P_5 = e_1^5 - 5^4 e_3(e_1^2 - 5e_2),$$

$$P_6 = e_1^6 - 2^2 \cdot 3 e_1^4 e_2 - 2 \cdot 3^4 \cdot 17 e_1^3 e_3 + 2^4 \cdot 3 e_1^2 e_2^2 - \\ - 2^3 \cdot 3^4 \cdot 19 e_1 e_2 e_3 - 2^6 e_2^3 + 3^3 \cdot 19^3 e_3^2,$$

$$P_7 = e_1^7 - 7^4 e_3(5e_1^4 - 2 \cdot 7^2 e_1^2 e_2 - 7^4 e_1 e_3 + 7^3 e_2^2),$$

$$P_{11} = e_1^{11} - 11^4 e_3(5 \cdot 53 e_1^8 - 2 \cdot 11^2 \cdot 197 e_1^6 e_2 - 11^3 \cdot 61 \cdot 1499 e_1^5 e_3 + \\ + 2 \cdot 11^4 \cdot 41 e_1^4 e_2^2 - 11^5 \cdot 17 \cdot 2957 e_1^3 e_2 e_3 - 5 \cdot 11^6 e_1^2 e_2^3 + \\ + 2 \cdot 11^6 \cdot 67^3 e_1 e_2^2 e_3 - 2^2 \cdot 7 \cdot 11^7 \cdot 67 e_1 e_2^2 e_3 + 11^7 e_2^4 - 11^7 \cdot 67^3 e_2 e_3^2).$$

Сопоставим числу n набор простых чисел, которые возникают как делители коэффициентов полиномов $P_n(e_1, e_2, e_3)$.

Вопрос:

Какие закономерности в этом сопоставлении?

Группы G_n и полиномы $p_n(z; x, y)$

Группы G_n и полиномы $p_n(z; x, y)$ возникают в различных областях математики и математической физики.

В работе В.М. Бухштабера, А.Н. Холодова, 1989, полиномы $p_n(z; x, y)$ описывают сдвиги T_x^y на **однородных коалгебрах** с собственными функциями $b_n(\lambda x)$, которые являются гипергеометрическими, где

$$T_x^y : Q[[x]] \rightarrow Q[[x, y]], \quad T_x^y b_n(x) = b_n(x)b_n(y),$$
$$b_n(x) = {}_0F_{n-1} \left(\frac{1}{n}, \dots, \frac{n-1}{n}; \frac{(n-1)!}{n^{n-1}} x \right).$$

Получаем:

$$b_1(x) = e^x, \quad b_2(x) = ch(\sqrt{2x}),$$

где $ch(x)$ – гиперболический косинус.

В работе I. Gaiur, V. Rubtsov, D. van Straten, 2024, описана связь полиномов $p_n(z; x, y)$ с **мультипликативными ядрами** в смысле Концевича, бесселевыми ядрами и потенциалами в модели Ландау–Гинзбурга.

Суммы Кронекера

Определение

Пусть A и B — произвольные квадратные матрицы над полем $\mathbb{C}$ порядков m и n соответственно и I_n, I_m — единичные матрицы.

Кронекеровой суммой $A \boxplus B$ матриц A и B называется $(mn \times mn)$ -матрица

$$A \boxplus B = A \otimes_{\mathbb{C}} I_n + I_m \otimes_{\mathbb{C}} B.$$

Суммы Кронекера используются в различных задачах теоретических и прикладных исследований, включая теорию дифференциальных уравнений, квантовые вычисления, машинное обучение, робототехнику.

Например, в терминах суммы Кронекера формулируется критерий существования и единственности решения матричного уравнения

$$AX + XB = C.$$

Собственные значения матриц и суммы Кронекера

Рассмотрим мультимножества $[\lambda_1, \dots, \lambda_m]$ и $[\mu_1, \dots, \mu_n]$ собственных значений матриц A и B .

Предложение (С. Stephanos, 1900)

Пусть $p(x, y) = \sum_{j,k=0}^{\ell} c_{jk} x^j y^k \in \mathbb{C}[x, y]$. Тогда

$$[p(\lambda_r, \mu_s), r = 1, \dots, m, s = 1, \dots, n] -$$

мультимножество собственных значений матрицы

$$p(A, B) = \sum_{j,k=0}^{\ell} c_{jk} A^j \otimes B^k.$$

Следствие

$[\lambda_r + \mu_s, r = 1, \dots, m, s = 1, \dots, n]$ – мультимножество собственных значений суммы Кронекера $A \boxplus B$.

Фробениусовы сопровождающие матрицы

Определение

Фробениусовой сопровождающей матрицей $F(a_{n-1}, \dots, a_0)$ полинома $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0 \in \mathbb{C}[t]$ называется матрица

$$\begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ 0 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Аналогично определяется Фробениусова сопровождающая блочная матрица $F(A_{n-1}, \dots, A_0)$ матричного полинома

$$f(t) = t^n + A_{n-1}t^{n-1} + \dots + A_0 \in \text{Mat}_m(\mathbb{C})[t].$$

Фробениусовы матрицы и суммы Кронекера

Введём характеристический полином $(n \times n)$ -матрицы A

$$\chi(t; A) = \det(tI_n - A),$$

где I_n – единичная $(n \times n)$ -матрица. Мультимножество корней полинома $\chi(t; A)$ совпадает с мультимножеством собственных значений матрицы A .

Пусть $f(t) = t^m + a_{m-1}t^{m-1} + \dots + a_0$. Тогда $\chi(t; F(a_{m-1}, \dots, a_0)) = f(t)$.

Предложение

Пусть $[\lambda_j]$ и $[\mu_k]$ – мультимножества корней полиномов

$$f(t) = t^m + a_{m-1}t^{m-1} + \dots + a_0 \text{ и } g(t) = t^n + b_{n-1}t^{n-1} + \dots + b_0.$$

Тогда $[\lambda_j + \mu_k]$ является мультимножеством корней характеристического полинома степени mn

$$\chi(t; F(a_{m-1}, \dots, a_0) \boxplus F(b_{n-1}, \dots, b_0)).$$

Предложение (В.М. Бухштабер, М.И. Корнев, 2025)

- (1) Для x, y, z и $t^n = z$ выполняется равенство

$$p_n(z; x, y) = \chi\left(t; \underbrace{F(0, \dots, 0, -x)}_n \boxplus \underbrace{F(0, \dots, 0, -y)}_n\right).$$

- (2) Полином $p_n(z; (-1)^n x, (-1)^n y)$ симметричен по переменным x, y и z .
- (3) $p_n(z; x, y)$ является однородным полиномом степени n с целыми коэффициентами по переменным x, y и z .

Великая теорема Ферма

Гипотеза (Р. Fermat, 1637)

Для любого **натурального числа** $n > 2$ уравнение $a^n + b^n = c^n$ не имеет решений в целых ненулевых числах a, b, c .

Положим $n = 2^u m$ – целое число, где $u \geq 0$, а m – нечётное.

В работах по великой проблеме Ферма рассматриваются два класса задач:

- I. Пусть a, b, c – ненулевые целые числа и $\gcd(m, abc) = 1$, тогда $a^n + b^n \neq c^n$.
- II. Пусть a, b, c – ненулевые попарно взаимно простые целые числа и $\gcd(m, abc) \neq 1$, тогда $a^n + b^n \neq c^n$.

Числа Софи Жермен (1776–1831)

Утверждение I было доказано Софи Жермен для $n = p$, где p – простое число, такое, что число $2p + 1$ также простое. Такие числа названы **числами Софи Жермен**.

Первые простые числа Софи Жермен (см. последовательность A005384):

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, ...

Предполагается, что количество простых чисел Софи Жермен бесконечно, но это **открытый вопрос**!

Числа Бернулли

Последовательность чисел Бернулли $\{B_0 = 1, B_1 = -\frac{1}{2}, B_2, \dots\}$ была введена Якобом Бернулли (1655–1705) в связи с вычислением сумм

$$\sum_{n=0}^{N-1} n^k = \frac{1}{k+1} \sum_{s=0}^k \binom{k+1}{s} B_s N^{k+1-s}.$$

Производящий ряд чисел Бернулли

$$\frac{x}{e^x - 1} = \sum_{s=0}^{\infty} B_s \frac{x^s}{s!}.$$

Теорема (Штаудта–Клаузена)

Число $B_{2s} + \sum_{(p-1)|2s} \frac{1}{p}$, где p – **простые числа**, является **целым**.

Следствие

Знаменатель рационального числа B_{2s} является произведением **простых чисел p** , таких, что $(p-1)$ является делителем числа $2s$.

Регулярные и иррегулярные простые числа

Простое число $p \geq 3$ называется **регулярным**, если числители всех чисел Бернулли $B_2, B_4, \dots, B_{p-3}$ не делятся на p .

Предполагается, что регулярных простых чисел бесконечно много, но это **открытый вопрос!**

Теорема (Е. Kummer, 1810-1893)

Если простое p регулярно, то уравнение $a^p + b^p = c^p$ не имеет решений в натуральных числах.

Простое число, не являющееся регулярным, называется **иррегулярным**.

Несколько первых иррегулярных простых чисел:

37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, ...

Теорема Вендта

Определение

Матрицей Вендта W_n называется циркулянт

$$W_n = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} \\ \binom{n}{n-1} & 1 & \binom{n}{1} & \cdots & \binom{n}{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \cdots & 1 \end{pmatrix}$$

Теорема (E. Wendt, 1894)

Пусть $p > 3$ – простое и $q = 2kp + 1$ – простое при некотором $k \geq 1$. Тогда существуют целые a, b, c , не делящиеся на q , такие, что

$$a^p + b^p + c^p \equiv 0 \pmod{q}$$

тогда и только тогда, когда q является делителем числа $\det W_{2k}$.

Теорема Жермен в форме Лежандра

Теорема

Пусть p и q — различные нечётные простые числа и выполняются следующие условия:

- (1) Если a, b, c — целые числа и $a^p + b^p + c^p \equiv 0 \pmod{q}$, то $q \mid abc$.
- (2) Не существует целого числа m , такого, что $m^p \equiv p \pmod{q}$.

Тогда утверждение I верно для показателя p .

Предложение

Если p и q — нечётные простые числа, и $q = 2pk + 1$ для натурального k , то условие (2) теоремы эквивалентно каждому из следующих утверждений:

- $(2k)^{2k} \not\equiv 1 \pmod{q}$;
- $p^{2k} \not\equiv 1 \pmod{q}$.

Разлагая число $\det W_{2k}$ на множители при помощи средств компьютерной алгебры, используя теорему Вендта, теорему Жермен в форме Лежандра и сформулированное выше предложение, получаем:

Предложение (G. Fee, A. Granville, 1991)

Пусть p и $2kp + 1$ – простые числа, где $k \leq 100$.
Тогда утверждение I выполняется для показателя p .

В работе [D. Ford, V. Jha, 1993] это предложение проверено для $k \leq 500$.

Матрицы $W_n(z; x, y)$

Определение

y -циркулянт $\text{Circ}_y(a_0, \dots, a_{n-1})$ называется матрица Теплица

$$\text{Circ}_y(a_0, \dots, a_{n-1}) = \begin{pmatrix} a_0 & ya_1 & ya_2 & \cdots & ya_{n-1} \\ a_{n-1} & a_0 & ya_1 & \ddots & \vdots \\ a_{n-2} & a_{n-1} & a_0 & \ddots & ya_2 \\ \vdots & \ddots & \ddots & \ddots & ya_1 \\ a_1 & \cdots & a_{n-2} & a_{n-1} & a_0 \end{pmatrix}$$

Определение (В.М. Бухштабер, М.И. Корнев, 2025)

Матрицей $W_n(z; x, y)$ называется y -циркулянт, у которого

$$a_0 = w^n + (-1)^{n+1}x + y, \quad a_k = \binom{n}{k}w^k, \quad k = 1, \dots, n-1, \quad w^n = z.$$

Группы $\mathbb{G}_n$ и матрицы Вендта W_n

Положим $w = t$.

Теорема (*) (В.М. Бухштабер, М.И. Корнев, 2025)

- (1) Полином $p_n(z; x, y)$, задающий сложение в n -значной группе $\mathbb{G}_n$, является детерминантом матрицы $W_n(z; x, y)$.
- (2) $W_n(1; (-1)^n x, 1) = W_n - tI_n$, где $t = x - 1$ и W_n – матрица Вендта.

Следствие

$$\chi(t, W_n) = p_n(x; (-1)^n, (-1)^n), \text{ где } t = (-1)^n x - 1,$$

$$W_n = W_n(1; (-1)^n, 1),$$

$$\det W_n = p_n((-1)^n; (-1)^n, (-1)^n).$$

Примеры

Положим $p_n = p_n(z; (-1)^n x, (-1)^n y)$ и $z = w^n$.

$$p_2 = \begin{vmatrix} w^2 - x + y & 2wy \\ 2w & w^2 - x + y \end{vmatrix}$$

$$p_3 = \begin{vmatrix} w^3 + x + y & 3yw & 3yw^2 \\ 3w^2 & w^3 + x + y & 3yw \\ 3w & 3w^2 & w^3 + x + y \end{vmatrix}$$

$$p_4 = \begin{vmatrix} w^4 - x + y & 4yw & 6yw^2 & 4yw^3 \\ 4w^3 & w^4 - x + y & 4yw & 6yw^2 \\ 6w^2 & 4w^3 & w^4 - x + y & 4yw \\ 4w & 6w^2 & 4w^3 & w^4 - x + y \end{vmatrix}$$

Характеристические полиномы и детерминанты матриц Вендта

Первые примеры полиномов $\chi(t, W_n)$, где $t = (-1)^n x - 1$:

$$n = 2 : x(x - 2^2), \det W_2 = -3$$

$$n = 3 : (x - 1)^2(x + 2^3), \det W_3 = 2^2 \cdot 7$$

$$n = 4 : x(x - 2^4)(x + 2^2)^2, \det W_4 = -3 \cdot 5^3$$

$$n = 5 : (x + 2^5)(x^2 - 11x - 1)^2, \det W_5 = 11^2 \cdot 31$$

$$n = 6 : x(x - 2^6)(x - 1)^2(x + 3^3)^2, \det W_6 = 0$$

$$n = 7 : (x + 2^7)(x^3 - 3 \cdot 19x^2 - 17^2x + 1)^2, \det W_7 = 2^6 \cdot 29^2 \cdot 127$$

$$n = 8 : x(x - 2^8)(x - 2^4)^2(x^2 + 2^3 \cdot 17x + 2^4)^2, \det W_8 = -3^7 \cdot 5^3 \cdot 17^3$$

Предложение (В.М. Бухштабер, М.И. Корнев, 2025)

Имеют место следующие утверждения:

- 1 $(-1)^n * (-1)^n$ является мультимножеством корней полинома $\chi(t, W_n)$, где $t = (-1)^n x - 1$.
- 2 $1 * 1$ является мультимножеством корней полинома $\chi(t, \widetilde{W}_n)$, где $\widetilde{W}_n - (-1)^n$ -циркулянт и $t = x + (-1)^{n+1}$.
- 3 $1 * (-1)^n$ является мультимножеством корней полинома $\chi(t, W_n)$, где $t = x - 1$.

Приложение теоремы Вольстенхольма

Теорема (В.М. Бухштабер, М.И. Корнев, 2025)

При простых $n \geq 5$ многочлен

$$p_n(z; (-1)^n x, (-1)^n y) - (x + y + z)^n$$

делится на n^4xyz .

Доказательство основывается на нашей теореме (*) и классическом результате:

Теорема (J. Wolstenholme, 1862)

Число

$$\binom{2n-1}{n-1} - 1$$

делится на n^3 для простых $n \geq 5$.

Простые числа Вольстенхольма

Определение

Простым числом Вольстенхольма называется простое число n , для которого $\binom{2n-1}{n-1} - 1$ делится на n^4 .

Простое число Вольстенхольма p является делителем числителя числа Бернулли B_{p-3} , т.е. является **иррегулярным простым числом**.

В настоящее время известны только два простых числа Вольстенхольма: 16 843 и 2 124 679. Следующее простое число Вольстенхольма, если оно существует, обязательно больше 10^{11} .

Теорема Вольстенхольма и числа Каталана

Определение

Числа $C_n = \frac{2n!}{n!(n+1)!}$ называются **числами Каталана** (1838).

$\{C_n\} = \{1, 2, 5, 14, 42, 132, 429, \dots\}$ – одна из наиболее известных последовательностей перечислительной комбинаторики.

Например, число C_n равно:

- количеству триангуляций выпуклого $(n+2)$ -угольника;
- количеству вершин ассоциэдра (многогранника Сташефа) $As^{n-1} \subset \mathbb{R}^{n-1}$.

Используя теорему Вольстенхольма, получаем:

Предложение

Число $(n+1)C_n - 2$ делится на n^3 , когда $n > 3$ – простое число, и делится на n^4 , когда n – простое число Вольстенхольма.

Группы $\mathbb{G}_n$ и суммы Кронекера

Итерации n -значного сложения в группах $\mathbb{G}_n$ приводят к полиномам

$$p_n(z; x_1, \dots, x_m) = \prod_{s_1, \dots, s_m=1}^n (\sqrt[n]{z} + \epsilon^{s_1} \sqrt[n]{x_1} + \dots + \epsilon^{s_m} \sqrt[n]{x_m}),$$

где ϵ – первообразный корень степени n из единицы.

Предложение

(1) Для $x_1, \dots, x_m$ и $t^n = z$ выполняется равенство

$$p_n(z; x_1, \dots, x_m) = \chi\left(t; \underbrace{F(0, \dots, 0, (-1)^{n+1}x_1)}_n \boxplus \dots \boxplus \underbrace{F(0, \dots, 0, (-1)^{n+1}x_m)}_n\right).$$

(2) Полиномы $p_n(z; x_1, \dots, x_m)$ симметричны по всем переменным.

(3) Полиномы $p_n(z; x_1, \dots, x_m)$ являются однородными полиномами степени n^{m-1} от $z, x_1, \dots, x_m$ с целыми коэффициентами.

Примеры полиномов $p_n = p_n(z; x_1, \dots, x_m)$

$m = 3$

$$p_1 = e_1,$$

$$p_2 = e_1^4 - 2^3(e_1^2 e_2 - 2e_2^2 + 2^3 e_4),$$

$$p_3 = e_1^9 - 3^4(e_1^6 e_3 - 3^3 e_1^3 e_3^2 + 3^5 e_3^3 - 2 \cdot 3^3 e_1^5 e_4 + 3^5 e_1^3 e_2 e_4 - 3^6 e_1^2 e_3 e_4).$$

$m = 4$

$$p_1 = e_1,$$

$$p_2 = e_1^8 - 2^4(e_1^6 e_2 - 2 \cdot 3e_1^4 e_2^2 + 2^4 e_1^2 e_2^3 - 2^4 e_2^4 + 2^3 e_1^4 e_4 - 2^6 e_1^2 e_2 e_4 + \\ + 2^7 e_2^2 e_4 - 2^8 e_4^2 + 2^7 e_1^3 e_5 - 2^9 e_1 e_2 e_5 + 2^{10} e_3 e_5).$$

Неприводимость полиномов $p_n(z; x_1, \dots, x_m)$

Введем матрицу Фробениуса $F(\underbrace{0, \dots, 0}_{n_j}, x_j)$ полинома $t^{n_j} = x_j$, поле $\mathbb{k}$ и

$$n = \text{НОК}(n_1, \dots, n_m), \quad e(\mathbb{k}) = \begin{cases} 1, & \text{если } \text{char } \mathbb{k} = 0, \\ \text{char } \mathbb{k}, & \text{иначе.} \end{cases}$$

Теорема (В.М. Бухштабер, М.И. Корнев, 2025)

Пусть $x_1, \dots, x_m$ – алгебраически независимые переменные и $n_1, \dots, n_m$ – натуральные числа. Тогда полином

$$q(\{n_i\}, \{x_j\}; t) = \chi\left(t; F(\underbrace{0, \dots, 0}_{n_1}, x_1) \boxplus \dots \boxplus F(\underbrace{0, \dots, 0}_{n_m}, x_m)\right)$$

от $t, x_1, \dots, x_m$ неприводим над полем $\mathbb{k}$, таким, что $\text{НОД}(n, e(\mathbb{k})) = 1$.

Следствие

Полиномы $p_n(z; x_1, \dots, x_m)$ неприводимы над $\mathbb{C}$ для всех натуральных n .

Радикалы пары натуральных чисел

Определение

- (1) **Радикалом** пары натуральных чисел (x, k) называется число $a = a(x, k) = x^{\frac{1}{k}}$.
- (2) **Показателем** радикала a называется наименьшее натуральное число n , такое, что a^n – натуральное число.

Предложение (Н. Ursell, 1974)

Пусть $a_1, \dots, a_m$ – радикалы с показателями $n_1, \dots, n_m$, такие, что натуральные числа $a_1^{n_1}, \dots, a_m^{n_m}$ попарно взаимно просты. Тогда числа $a_1, \dots, a_m$ порождают расширение степени $n_1 \cdots n_m$ поля $\mathbb{Q}$.

Неприводимость полиномов $q(\{n_i\}, \{x_i\}; t)$ над $\mathbb{Q}$

Рассмотрим множество пар натуральных чисел $\{(x_1, k_1), \dots, (x_m, k_m)\}$, где числа $x_1, \dots, x_m$ попарно взаимно просты.

Введем множество $\{n_1, \dots, n_m\}$ показателей радикалов $\{x_1^{\frac{1}{k_1}}, \dots, x_m^{\frac{1}{k_m}}\}$.

Теорема (В.М. Бухштабер, М.И. Корнев, 2025)

Полином

$$q(\{n_i\}, \{x_i\}; t) = \chi\left(t; \underbrace{F(0, \dots, 0, x_1)}_{n_1} \boxplus \dots \boxplus \underbrace{F(0, \dots, 0, x_m)}_{n_m}\right)$$

степени $n_1 \cdots n_m$ от переменной t неприводим над $\mathbb{Q}$.

Неприводимость полиномов $p_n(z)$ над $\mathbb{Q}$

Рассмотрим множество $\{x_1, \dots, x_m\}$ натуральных попарно взаимно простых чисел, таких, что показатель радикала $x_j^{\frac{1}{n}}$ равен фиксированному натуральному числу n для всех $j = 1, \dots, m$.

Следствие

Полином $p(z; x_1, \dots, x_m)$ степени n^{m-1} от переменной $z = t^n$ неприводим над $\mathbb{Q}$.



В.М.Бухштабер, С.П.Новиков,
Формальные группы, степенные системы и операторы Адамса.
Матем. Сб., 84(126):1 (1971), 81–118.



В.М.Бухштабер,
Двузначные формальные группы. Алгебраическая теория и приложения
к кобордизмам. I; II.
Изв. АН СССР. Сер. матем., 39:5, 1975, 1044–1064; 40:2, 1976, 289–325.



В.М.Бухштабер, А.Н.Холодов,
Группы формальных диффеоморфизмов суперпрямой, производящие
функции для последовательностей полиномов и функциональные
уравнения.
Изв. АН СССР, сер. мат., 53:5, М., 1989, 944–970.



V.M.Buchstaber,
 n -valued groups: theory and applications.
Moscow Math. J., 6:1, 2006, 57–84.



P.Lancaster, M.Tismenetsky,
The Theory of Matrices: With Applications.
Computer Science and Scientific Computing. Elsevier Science, 1985.



P.Ribenboim,
Fermat's Last Theorem for Amateurs.
Springer New York, NY, 1st edition, 1999.



H.D.Ursell,
The degrees of radical extensions.
Canadian Mathematical Bulletin, 17(4) (1974), 615–617.



E.Wendt,
Arithmetische Studien über den 'letzten' Fermatschen Satz, welcher aussagt,
dass die Gleichung $a^n = b^n + c^n$ für $n > 2$; in ganzen Zahlen nicht auflösbar ist.
Journal für die reine und angewandte Mathematik, 113, 1894, 335–347.



J.Wolstenholme,
On certain properties of prime numbers.
The Quarterly Journal of Pure and Applied Mathematics, 5 (1862), 35–39.



V.M.Buchstaber, A.P.Veselov,
Integrable correspondences and algebraic representations of multivalued groups.
Internat. Math. Res. Notices, N 8, 1996, 381–400.



В.М.Бухштабер, А.П.Веселов,
Топограф Конвея, $PGL_2(\mathbb{Z})$ -динамика и двузначные группы.
УМН, 74:3(447), 2019, 17–62.



I.Gaiur, V.Rubtsov, D.van Straten,
Product formulas for the Higher Bessel functions.
arXiv:2405.03015v1 [math.AG] 5 May 2024.



Victor Buchstaber, Mikhail Kornev,
 n -Valued Groups, Kronecker Sums, and Wendt's (x, y, z) -Matrices.
arXiv:2505.04296v1 [math.GR] 7 May 2025.