Math-Net.Ru

Общероссийский математический портал

В. Л. Куракин, Алгебры Хопфа линейных рекуррентных последовательностей, *Дискрет. матем.*, 2004, том 16, выпуск 2, 7–43

DOI: <https://doi.org/10.4213/dm150>

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: 54.80.73.141

26 апреля 2023 г., 11:00:49

Алгебры Хопфа линейных рекуррентных последовательностей

© 2004 г. В. Л. Куракин

Алгебра линейных рекуррентных последовательностей над коммутативным кольцом R является алгеброй Хопфа, дуальной к алгебре многочленов над кольцом R . В работе рассматривается ряд понятий и операций из теории алгебр и модулей Хопфа, которые получают интересную интерпретацию в терминах линейных рекуррентных последовательностей.

Работа выполнена при поддержке грантами Президента Российской Федерации МД-2452.2004.10 поддержки молодых ученых и НШ-2358.2003.9 поддержки ведущих научных школ.

1. Введение

Пусть R — коммутативное кольцо с единицей, ${}_R M$ — левый модуль над R . Последовательностью над M назовем произвольную функцию $u: \mathbb{N}_0 \rightarrow M$. Последовательность $u = (u(0), u(1), \dots)$ называется линейной рекуррентной последовательностью (ЛРП) порядка m над модулем M , если существуют элементы $c_0, \dots, c_{m-1} \in R$ такие, что

$$u(i+m) = c_{m-1}u(i+m-1) + \dots + c_1u(i+1) + c_0u(i), \quad i \geq 0. \quad (1)$$

Многочлен

$$F(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0 \in R[x]$$

называется характеристическим многочленом ЛРП u , а вектор

$$u(0, m-1) = (u(0), \dots, u(m-1)) \in M^m$$

— ее начальным вектором. Множество всех ЛРП над модулем M с характеристическим многочленом $F(x)$ обозначается через $L_M(F)$. Множество всех ЛРП над модулем M обозначается $\mathcal{L}M^{(1)}$, а множество всех последовательностей над M обозначается $M^{(1)}$. Многочлен $F(x)$ будем называть реверсивным, если его свободный член $F(0)$ является обратимым элементом кольца R . ЛРП называется реверсивной, если у нее существует реверсивный характеристический многочлен. Множество всех реверсивных ЛРП над M обозначим $\mathcal{L}M_{\text{rev}}^{(1)}$.

Впервые алгебра линейных рекуррентных последовательностей над полем P интерпретирована как алгебра Хопфа, дуальная к алгебре многочленов $P[x]$, в [22]. Операция умножения в этой алгебре есть конволюция последовательностей. В [15] показано, что

на пространстве линейных рекуррентных последовательностей над полем структуру биалгебры можно ввести в точности двумя различными способами, при которых умножение последовательностей задается как их конволюция или покоординатное произведение. Операция конволюции ЛРП изучалась независимо в [4] и [15], покоординатное произведение ЛРП исследовалось значительно ранее в [27]. Еще одна операция конволюции ЛРП, не связанная с алгебрами Хопфа, изучалась в [16]. Подалгебры алгебры Хопфа $\mathcal{L}P^{(1)}$ исследованы в [5]. В [13] показано, что алгебра Хопфа, дуальная к алгебре $P[x_1, \dots, x_k]$ многочленов от k переменных над полем P , является алгеброй $\mathcal{L}P^{(k)}$ всех k -линейных рекуррентных последовательностей (см. ниже раздел 8). Алгебры Хопфа ЛРП над полем рассматривались также в [17, 20, 25, 26].

В [6, 7] доказано, что алгебра линейных рекуррентных последовательностей над произвольным коммутативным кольцом R есть корректно определенная алгебра Хопфа, дуальная к алгебре многочленов над R . В [11] этот результат независимо получен для алгебры многочленов над коммутативным нетеровым кольцом (отметим, однако, что над коммутативным нетеровым кольцом дуальная алгебра Хопфа A° существует и определена корректно не только для алгебры многочленов, но и для произвольной алгебры Хопфа A , см. [1]). Целью данной, во многом обзорной, статьи является более подробное изложение и развитие указанных результатов.

На алгебре многочленов $R[x]$ (с обычной операцией умножения многочленов) можно задать две различные структуры коалгебры, относительно которых $R[x]$ превращается в алгебру Хопфа $R[x]$ или в биалгебру $R[x]^\bullet$. Точка в обозначениях показывает, что на одном и том же множестве заданы различные структуры биалгебр. Дуальные алгебры Хопфа $R[x]^\circ$ и биалгебра $R[x]^\circ$ оказываются алгеброй Хопфа $\mathcal{L}R^{(1)}$ и биалгеброй $\mathcal{L}R^{(1)\bullet}$ линейных рекуррентных последовательностей, в которых умножение задается соответственно как конволюция и покоординатное произведение последовательностей, а структуры коалгебр одинаковы. Если биалгебру $R[x]^\bullet$ расширить до биалгебры $R[x, x^{-1}]^\bullet$ многочленов Лорана, то в последней можно задать антипод. Дуальная алгебра Хопфа $R[x, x^{-1}]^\circ$ есть алгебра $\mathcal{L}R_{bi}^{(1)\bullet}$ линейных рекуррентных бипоследовательностей над кольцом R , которая оказывается изоморфной подалгебре Хопфа $\mathcal{L}R_{rev}^{(1)\bullet}$ реверсивных последовательностей в биалгебре $\mathcal{L}R^{(1)\bullet}$.

Основные понятия, связанные с алгебрами Хопфа, можно найти в работах [1, 2, 10, 21, 24]. Линейные рекуррентные последовательности над полями рассматриваются в [8, 9], а над кольцами и модулями — в [3, 17, 18]. Ниже мы приводим все необходимые определения и свойства (без доказательства) и излагаем материал достаточно подробно так, чтобы текст был понятен для читателя, не знакомого с алгебрами Хопфа и линейными рекуррентами. Мы надеемся, что введение различных алгебраических структур на множестве линейных рекуррентных последовательностей поможет более полно понять закономерности их строения, а также послужит хорошим содержательным примером при изучении алгебр Хопфа.

2. Алгебры Хопфа и дуальные алгебры

Всюду ниже R — коммутативное кольцо с единицей 1. Термин отображение в дальнейшем означает R -линейное отображение, то есть гомоморфизм R -модулей, Hom и $\otimes$ означают Hom_R и $\otimes_R$ соответственно. Через 1_A обозначается тождественное отображение $A \rightarrow A$. Каждый R -модуль A будем отождествлять с модулями $R \otimes A$ и $A \otimes R$. Когда подобные отождествления используются внутри формул, знак равенства $=$ будем заменять знаком $\equiv$

равенства с точностью до некоторого отождествления (например, см. ниже определения единицы алгебры и коединицы коалгебры).

Каждую алгебру можно рассматривать как R -модуль A с операцией умножения m и единицей e , которые являются отображениями, удовлетворяющими законам ассоциативности и унитарности соответственно:

$$\begin{aligned} m &= m_A: A \otimes A \rightarrow A, & m(m \otimes 1_A) &= m(1_A \otimes m), \\ e &= e_A: R \rightarrow A, & m(e \otimes 1_A) &\equiv m(1_A \otimes e) \equiv 1_A. \end{aligned}$$

Другими словами, коммутативны диаграммы

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{1_A \otimes m} & A \otimes A \\ m \otimes 1_A \downarrow & & \downarrow m \\ A & \xrightarrow{m} & A \end{array} \quad \begin{array}{ccccc} R \otimes A & \longleftrightarrow & A & \longleftrightarrow & A \otimes R \\ e \otimes 1_A \downarrow & & \downarrow 1_A & & \downarrow 1_A \otimes e \\ A \otimes A & \xrightarrow{m} & A & \xleftarrow{m} & A \otimes A \end{array}$$

где $\longleftrightarrow$ означает отождествление. Единичным элементом алгебры A является элемент $e(1)$, который также обозначается символом 1 . Алгебра A коммутативна тогда и только тогда, когда $mt = m$, где $t: A \otimes A \rightarrow A \otimes A, a \otimes b \rightarrow b \otimes a$, — отображение перестановки. Результат применения операции умножения записывается в виде $m(a \otimes b) = ab$.

Коалгеброй называется R -модуль C с операциями (отображениями) коумножения Δ и коединицей ε , которые удовлетворяют законам коассоциативности и коунитарности:

$$\begin{aligned} \Delta &= \Delta_C: C \rightarrow C \otimes C, & (\Delta \otimes 1_C)\Delta &= (1_C \otimes \Delta)\Delta, \\ \varepsilon &= \varepsilon_C: C \rightarrow R, & (\varepsilon \otimes 1_C)\Delta &\equiv (1_C \otimes \varepsilon)\Delta \equiv 1_C. \end{aligned}$$

Другими словами, коммутативны диаграммы

$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ \Delta \downarrow & & \downarrow \Delta \otimes 1_C \\ C \otimes C & \xrightarrow{1_C \otimes \Delta} & C \otimes C \otimes C \end{array} \quad \begin{array}{ccccc} C \otimes C & \xleftarrow{\Delta} & C & \xrightarrow{\Delta} & C \otimes C \\ \varepsilon \otimes 1_C \downarrow & & \downarrow 1_C & & \downarrow 1_C \otimes \varepsilon \\ R \otimes C & \longleftrightarrow & C & \longleftrightarrow & C \otimes R \end{array}$$

Понятие коалгебры двойственно понятию алгебры, и диаграммы для коалгебры получаются из диаграмм для алгебры обращением стрелок. Результат применения коумножения Δ к элементу $c \in C$ принято записывать в виде

$$\Delta c = \sum_c c_{(1)} \otimes c_{(2)}, \quad c_{(i)} \in C, \quad i = 1, 2. \quad (2)$$

В этих обозначениях законы коассоциативности и коунитарности таковы:

$$\begin{aligned} \sum_c \Delta c_{(1)} \otimes c_{(2)} &= \sum_c c_{(1)} \otimes \Delta c_{(2)}, \\ \sum_c \varepsilon(c_{(1)}) c_{(2)} &= c = \sum_c c_{(1)} \varepsilon(c_{(2)}). \end{aligned}$$

Коалгебра C называется кокоммутативной, если $t\Delta = \Delta$, где $t: C \otimes C \rightarrow C \otimes C$ — отображение перестановки.

В дальнейшем алгебру мы будем обозначать (A, m, e) или $(A, \cdot, 1)$, а коалгебру — (C, Δ, ε) . Мы будем рассматривать только коммутативные алгебры и кокоммутативные коалгебры, поэтому термин (ко)алгебра ниже означает (ко)коммутативная (ко)алгебра.

Биалгеброй называется алгебра (A, m, e) , на которой задана структура коалгебры (A, Δ, ε) так, что

(1) $\Delta: A \rightarrow A \otimes A$ — гомоморфизм R -алгебр и

(2) $\varepsilon: A \rightarrow R$ — гомоморфизм R -алгебр.

Таким образом,

$$\begin{aligned}\Delta(ab) &= \Delta(a)\Delta(b), & \Delta(1) &= 1 \otimes 1, \\ \varepsilon(ab) &= \varepsilon(a)\varepsilon(b), & \varepsilon(1) &= 1,\end{aligned}$$

где $a, b \in A$. Биалгебра обозначается $(A, m, e, \Delta, \varepsilon)$.

Антиподом в биалгебре A называется отображение S , удовлетворяющее следующему условию:

$$S: A \rightarrow A, \quad m(S \otimes 1_A)\Delta = e\varepsilon = m(1_A \otimes S)\Delta.$$

Таким образом, коммутативна диаграмма

$$\begin{array}{ccccc} A \otimes A & \xleftarrow{\Delta} & A & \xrightarrow{\Delta} & A \otimes A \\ \downarrow S \otimes 1_A & & \downarrow \varepsilon & & \downarrow 1_A \otimes S \\ & & R & & \\ & & \downarrow e & & \\ A \otimes A & \xrightarrow{m} & A & \xleftarrow{m} & A \otimes A \end{array}$$

В обозначениях (2) аксиома антипода записывается в виде

$$\sum_c S(c_{(1)})c_{(2)} = \varepsilon(c)1 = \sum_c c_{(1)}S(c_{(2)}).$$

Биалгебра с антиподом называется алгеброй Хопфа.

R -подмодуль L алгебры (A, m, e) называется подалгеброй, если $m(L \otimes L) \subseteq L$ и $e(R) \subseteq L$. R -подмодуль L коалгебры (C, Δ, ε) называется подкоалгеброй, если $\Delta(L) \subseteq L \otimes L$. Подалгебра L биалгебры A , являющаяся подкоалгеброй, называется подбиалгеброй. Если к тому же A — алгебра Хопфа с антиподом S и $S(L) \subseteq L$, то L называется подалгеброй Хопфа в A .

Пример 1. На алгебре $(R[x], \cdot, 1)$ многочленов над кольцом R можно ввести структуру алгебры Хопфа $R[x] = (R[x], \cdot, 1, \Delta_x, \varepsilon_x, S_x)$, полагая

$$\Delta_x(F) = F(x \otimes 1 + 1 \otimes x), \quad \varepsilon_x(F) = F(0), \quad S_x(F) = F(-x), \quad F \in R[x],$$

а также структуру биалгебры $R[x]^* = (R[x], \cdot, 1, \Delta_x^*, \varepsilon_x^*)$, полагая

$$\Delta_x^*(F) = F(x \otimes x), \quad \varepsilon_x^*(F) = F(1), \quad F \in R[x].$$

Можно показать, что на биалгебре $R[x]^*$ невозможно задать антипод. Чтобы ввести на биалгебре $R[x]^*$ структуру алгебры Хопфа, рассмотрим ее как подалгебру в алгебре $R[x, x^{-1}]$ многочленов Лорана вида

$$F(x) = \sum_{s=-m}^n a_i x^i, \quad a_i \in R, \quad i = -m, -m+1, \dots, n,$$

где $m, n \in \mathbb{N}_0$.

Введем структуру алгебры Хопфа $R[x, x^{-1}]^* = (R[x, x^{-1}], \cdot, 1, \Delta_x^*, \varepsilon_x^*, S_x^*)$, полагая

$$\Delta_x^*(F) = F(x \otimes x), \quad \varepsilon_x^*(F) = F(1), \quad S_x^*(F) = F(x^{-1}), \quad F \in R[x, x^{-1}].$$

Таким образом, $\Delta_x^*(x^i) = x^i \otimes x^i$ и $S_x^*(x^i) = x^{-i}$, $i \in \mathbb{Z}$. При этом $R[x]^*$ — подбиалгебра в алгебре Хопфа $R[x, x^{-1}]^*$. Проверка того, что введенные операции удовлетворяют определениям, проводится непосредственно.

Элемент a коалгебры A называется групповым, если $\Delta a = a \otimes a$ и $\varepsilon(a) = 1$. Множество групповых элементов обозначается $G(A)$. Если A — биалгебра, то $G(A)$ замкнуто относительно умножения и является подполугруппой в $(A, \cdot)$. В алгебре Хопфа $G(A)$ — группа, причем $a^{-1} = S(a)$, $a \in G(A)$. Если A — биалгебра с единицей 1, то элемент $a \in A$ называется примитивным, если $\Delta a = a \otimes 1 + 1 \otimes a$. Множество $P(A)$ примитивных элементов является подгруппой в $(A, +)$. На алгебре многочленов $R[x]$ структура биалгебры определяется значениями Δx и $\varepsilon(x)$, поскольку $\Delta(x^n) = (\Delta x)^n$ и $\varepsilon(x^n) = (\varepsilon x)^n$. В приведенном выше примере две структуры биалгебры на $R[x]$ задаются так, что x оказывается примитивным или групповым элементом соответственно.

Пример 2. Пусть $R[x] = R[x_1, \dots, x_k]$ — алгебра многочленов от k переменных над кольцом R . Введем на ней структуру алгебры Хопфа $R[x] = (R[x], \cdot, 1, \Delta_x, \varepsilon_x, S_x)$ и биалгебры $R[x]^* = (R[x], \cdot, 1, \Delta_x^*, \varepsilon_x^*)$ с операциями

$$\begin{aligned} \Delta_x(F) &= F(x \otimes 1 + 1 \otimes x) = F(x_1 \otimes 1 + 1 \otimes x_1, \dots, x_k \otimes 1 + 1 \otimes x_k), \\ \Delta_x^*(F) &= F(x \otimes x) = F(x_1 \otimes x_1, \dots, x_k \otimes x_k), \\ \varepsilon_x(F) &= F(0), \\ \varepsilon_x^*(F) &= F(1), \\ S_x(F) &= F(-x), \end{aligned} \tag{3}$$

где $F(x) \in R[x]$, $0 = (0, \dots, 0)$, $1 = (1, \dots, 1) \in \mathbb{N}_0^k$.

Пусть $R[x, x^{-1}]$ — алгебра многочленов вида

$$F(x) = \sum_{s \in \mathbb{Z}^k} c_s x^s,$$

где лишь конечное число коэффициентов $c_s \in R$ отличны от 0. На этой алгебре можно ввести структуру алгебры Хопфа $(R[x, x^{-1}], \cdot, 1, \Delta_x^*, \varepsilon_x^*, S_x^*)$, в которой Δ_x^* и ε_x^* определяются так же, как в (3), и

$$S_x^*(F) = F(x^{-1}) = F(x_1^{-1}, \dots, x_k^{-1}), \quad F \in R[x, x^{-1}].$$

Отметим, что естественные отображения

$$R[x] \otimes \dots \otimes R[x] \rightarrow R[x], \quad R[x, x^{-1}] \otimes \dots \otimes R[x, x^{-1}] \rightarrow R[x, x^{-1}],$$

задаваемые правилом

$$F_1(x_1) \otimes \dots \otimes F_k(x_k) \rightarrow F_1(x_1) \dots F_k(x_k),$$

являются изоморфизмами биалгебр.

Данная работа посвящена изучению биалгебр и алгебр Хопфа, дуальных к алгебрам многочленов из примеров 1 и 2. Дадим определения дуальной коалгебры и дуальной алгебры.

Пусть (C, Δ, ε) — коалгебра. На дуальном R -модуле $C^* = \text{Hom}(C, R)$ зададим структуру алгебры. Операция умножения на C^* , обозначаемая $*$ или m , определяется следующим образом: если $u, v \in C^*$, то

$$u * v = m_R(u \otimes v) \Delta, \quad (4)$$

где $m_R: R \otimes R \rightarrow R$ — умножение в кольце R , $u \otimes v: C \otimes C \rightarrow R \otimes R$ — тензорное произведение гомоморфизмов. Таким образом, при условии (2)

$$(u * v)(c) = \sum_c u(c_{(1)})v(c_{(2)}). \quad (5)$$

Единичным элементом алгебры C^* является коединица ε коалгебры C . Соответственно, единичное отображение e определяется соотношением

$$e: R \rightarrow C^*, \quad e(1) = \varepsilon. \quad (6)$$

Полученная алгебра $(C^*, *, \varepsilon) = (C^*, m, e)$ называется конволютивной алгеброй коалгебры C . Операция умножения в этой алгебре часто называется конволюцией.

Операции конволютивной алгебры C^* получаются как дуализация операций исходной коалгебры C . Действительно, рассмотрим отображения, дуальные к коумножению $\Delta: C \rightarrow C \otimes C$ и коединице $\varepsilon: C \rightarrow R$:

$$\Delta^*: (C \otimes C)^* \rightarrow C^*, \quad \varepsilon^*: R^* \rightarrow C^*.$$

Они определяются обычным образом: если $\varphi \in (C \otimes C)^*$, $\psi \in R^*$, то

$$\Delta^*(\varphi) = \varphi \Delta: C \xrightarrow{\Delta} C \otimes C \xrightarrow{\varphi} R, \quad \varepsilon^*(\psi) = \psi \varepsilon: C \xrightarrow{\varepsilon} R \xrightarrow{\psi} R$$

Отображения Δ^* , ε^* еще не являются операциями алгебры C^* , поскольку не имеют нужной области определения. Пусть

$$\alpha: C^* \otimes C^* \rightarrow (C \otimes C)^*, \quad \beta: R \rightarrow R^*$$

— естественные гомоморфизм и изоморфизм, действующие следующим образом:

$$\alpha(u \otimes v) = m_R(u \otimes v), \quad \beta(r) = \hat{r} \in R^*, \quad \hat{r}(r') = rr',$$

где $r, r' \in R$, причем $\alpha(u \otimes v)$ — значение α в точке $u \otimes v$, в то время как $m_R(u \otimes v)$ — композиция отображений $u \otimes v$ и m_R . Таким образом, $\alpha(u \otimes v)(c \otimes c') = u(c)v(c')$ при

$c, c' \in C$, и β — канонический изоморфизм между R и R^* , сопоставляющий элементу $r \in R$ гомотетию $\hat{r} \in R^*$. Определим композиции

$$m = \Delta^* \alpha, \quad e = \varepsilon^* \beta.$$

Тогда

$$\begin{aligned} m(u \otimes v) &= \Delta^*(\alpha(u \otimes v)) = \Delta^*(m_R(u \otimes v)) = m_R(u \otimes v)\Delta, \\ e(1) &= \varepsilon^*(\beta(1)) = \varepsilon^*(\hat{1}) = \hat{1}\varepsilon = \varepsilon, \end{aligned}$$

то есть отображения m и e есть в точности операции конволютивной алгебры C^* .

Рассмотрим двойственную ситуацию. Пусть (A, m, e) — алгебра, и пусть $A^* = \text{Hom}(A, R)$. Ядро $\text{Ker } u$ отображения $u \in A^*$ является R -подмодулем в A . В модуле A^* рассмотрим подмодуль A° , состоящий из тех отображений u , ядро которых содержит идеал I кольца A (напомним, что A коммутативно) такой, что A/I есть конечно порожденный проективный R -модуль. Таким образом,

$$A^\circ = \{u \in A^* : \text{Ker } u \supseteq I, I \triangleleft A, A/I \in \mathbf{P}(R)\}, \quad (7)$$

где $\mathbf{P}(R)$ — множество конечно порожденных проективных R -модулей. Предположим, что ограничение определенного выше отображения $\alpha : A^* \otimes A^* \rightarrow (A \otimes A)^*$ на множество $A^\circ \otimes A^\circ$ является изоморфизмом $A^\circ \otimes A^\circ \cong (A \otimes A)^\circ$, который будем считать отождествлением. Определим на A° структуру коалгебры $(A^\circ, \Delta, \varepsilon)$. Если $u \in A^\circ$, то элемент $\Delta u \in A^\circ \otimes A^\circ$ определим следующим условием:

$$\Delta u = \sum_i u_{(1)} \otimes u_{(2)} \iff \sum_i u_{(1)}(a)u_{(2)}(b) = u(ab), \quad a, b \in A. \quad (8)$$

Эти условия задают Δu однозначно, поскольку, ввиду равенства $A^\circ \otimes A^\circ = (A \otimes A)^\circ$, каждый элемент из $A^\circ \otimes A^\circ$ однозначно определяется своими значениями в точках $a \otimes b$, $a, b \in A$. Кратко определение коумножения записывается в виде

$$\Delta u(a \otimes b) \equiv u(ab), \quad a, b \in A, \quad (9)$$

где использовано отождествление $R \otimes R \equiv R$. Данные определения задают условия, однозначно определяющие элемент Δu , но не дают явного описания Δu , то есть элементов $u_{(1)}, u_{(2)}$ в соотношении (8). Коединицу $\varepsilon : A^\circ \rightarrow R$ зададим соотношением

$$\varepsilon(u) = u(1), \quad u \in A^\circ, \quad 1 \in R. \quad (10)$$

Тогда $(A^\circ, \Delta, \varepsilon)$ — коалгебра, называемая коалгеброй, дуальной к алгебре A .

Покажем, что операции коалгебры A° дуальны к операциям алгебры A , и поясним, почему дуальные операции задаются на множестве A° меньшем, чем A^* . Отображения, дуальные к умножению $m : A \otimes A \rightarrow A$ и единице $e : R \rightarrow A$, имеют вид

$$\begin{aligned} m^* : A^* &\rightarrow (A \otimes A)^*, \quad m^*(\varphi) = \varphi m, \\ e^* : A^* &\rightarrow R^*, \quad e^*(\varphi) = \varphi e, \quad \varphi \in A^*. \end{aligned}$$

В общем случае образ отображения m^* не лежит в $\alpha(A^* \otimes A^*)$, что не позволяет рассматривать m^* как коумножение на A^* . В то же время, для подмножества $A^\circ \subseteq A^*$ выполняется

включение $m^*(A^\circ) \subseteq (A \otimes A)^\circ = A^\circ \otimes A^\circ$, причем m^* удовлетворяет закону коассоциативности на A° . Рассмотрим естественное отождествление $\beta^{-1}: R^* \rightarrow R$, $\beta^{-1}(\hat{r}) = r = \hat{r}(1)$, где $r, 1 \in R$. Тогда для любых $u \in A^\circ$, $a, b \in A$

$$\begin{aligned} m^*(u)(a \otimes b) &= (um)(a \otimes b) = u(ab), \\ \beta^{-1}e^*(u) &= \beta^{-1}(ue) = (ue)(1) = u(e(1)) = u(1), \end{aligned}$$

где 1 в выражении $u(1)$ означает единицу алгебры A , а в двух предыдущих выражениях — единицу кольца R . Сравнивая с соотношениями (9) и (10), получаем, что операции дуальной коалгебры $(A^\circ, \Delta, \varepsilon)$ совпадают, с точностью до отождествлений α и β , с отображениями m^* , e^* , дуальными к операциям алгебры A .

Указанное выше предположение о том, что $\alpha: A^\circ \otimes A^\circ \rightarrow (A \otimes A)^\circ$ — изоморфизм, выполнено по крайней мере в двух случаях: если кольцо R нетерово (см. [1]) или если A — алгебра многочленов $R[x]$ или $R[x, x^{-1}]$ над коммутативным кольцом R (см. [7]). Отметим, что в [1] при определении коалгебры, дуальной к алгебре, пропущено условие нетеровости кольца R .

Пусть $(A, m_A, e_A, \Delta_A, \varepsilon_A)$ — биалгебра. Предположим, что кольцо R нетерово, или что A — биалгебра многочленов $R[x]$ или $R[x, x^{-1}]$ над произвольным коммутативным кольцом R . Тогда определены конволютивная алгебра (A^*, m, e) коалгебры $(A, \Delta_A, \varepsilon_A)$ и коалгебра $(A^\circ, \Delta, \varepsilon)$, дуальная к алгебре (A, m_A, e_A) . При этом $m(A^\circ \otimes A^\circ) \subseteq A^\circ$, то есть A° — подалгебра в A^* , и $(A^\circ, m, e, \Delta, \varepsilon)$ — биалгебра, называемая дуальной к биалгебре A . Если дополнительно A — алгебра Хопфа с антиподом $S_A: A \rightarrow A$, то A° оказывается алгеброй Хопфа с антиподом

$$S: A^\circ \rightarrow A^\circ, \quad S^\circ(u) = uS_A, \quad (11)$$

являющимся ограничением отображения $S_A^*: A^* \rightarrow A^*$, дуального к S_A , на множество A° . В этом случае A называется алгеброй Хопфа, дуальной к A . Корректность операций дуальной биалгебры (алгебры Хопфа) следует из [1, 7].

3. Последовательности и бипоследовательности

Для последовательности $u \in M^{(1)}$ обозначим через $x^s u = (u(s), u(s+1), \dots)$ сдвиг u на s шагов влево. Определим умножение многочлена

$$F(x) = \sum_{s \geq 0} c_s x^s \in R[x]$$

на последовательность $u \in M^{(1)}$ как последовательность $F(x)u \in M^{(1)}$ вида

$$F(x)u = \sum_s c_s x^s u, \quad \text{то есть} \quad (F(x)u)(i) = \sum_s c_s u(i+s), \quad i \geq 0. \quad (12)$$

Эта внешняя операция задает на абелевой группе $(M^{(1)}, +)$ структуру левого $R[x]$ -модуля [17]. Легко увидеть, что u — ЛРП с характеристическим многочленом $F(x)$ тогда и только тогда, когда $F(x)$ унитарен и $F(x)u = 0$. Идеал

$$\text{An}(u) = \{F(x) \in R[x]: F(x)u = 0\} \triangleleft R[x]$$

назовем аннулятором последовательности $u \in M^{(1)}$. Идеал кольца $R[x]$ назовем унитарным, если он содержит унитарный многочлен. Очевидно, u есть ЛРП над M тогда и только тогда, когда идеал $\text{An}(u)$ унитарен.

Каждое отображение $\hat{u} \in R[x]^* = \text{Hom}(R[x], R)$ однозначно определяется своими значениями $\hat{u}(1) = \hat{u}(x^0), \hat{u}(x), \hat{u}(x^2), \dots$. Сопоставим этому отображению последовательность $u \in R^{(1)}$ со знаками

$$u(i) = \hat{u}(x^i), \quad i \geq 0.$$

Тогда отображение $R[x]^* \rightarrow R^{(1)}, \hat{u} \rightarrow u$, является изоморфизмом R -модулей, в дальнейшем часто рассматриваемым как отождествление

$$R[x]^* \equiv R^{(1)}. \quad (13)$$

Структура левого $R[x]$ -модуля на $R^{(1)}$ индуцирует, с помощью (13), структуру левого $R[x]$ -модуля на $R[x]^*$ согласно правилу

$$F(x)\hat{u} = \hat{u}\hat{F}, \quad \text{то есть} \quad (F(x)\hat{u})(G) = \hat{u}(FG), \quad G \in R[x], \quad (14)$$

где $\hat{F}: R[x] \rightarrow R[x]$ — оператор умножения на F (гомотетии). Легко проверить непосредственно, что

$$\hat{u}(F) = (F(x)u)(0), \quad F \in R[x].$$

Следовательно, $F(x)u = 0$ тогда и только тогда, когда $\hat{u}(x^i F) = 0$ для всех $i \geq 0$, то есть

$$F(x) \in \text{An}(u) \iff F(x)R[x] \subseteq \text{Ker } \hat{u}. \quad (15)$$

В частности, $\text{An}(u)$ содержит унитарный многочлен тогда и только тогда, когда $\text{Ker } \hat{u}$ содержит унитарный идеал. Отметим, что R -модуль $\text{Ker } \hat{u} \subseteq R[x]$ в общем случае значительно шире идеала $\text{An}(u) \triangleleft R[x]$. Например, если $u = (0, 1, 0, 1, \dots)$, то $\text{An}(u) = (x^2 - 1)R[x]$, тогда как $\text{Ker } \hat{u}$ содержит произвольный многочлен $G(x^2)$, поскольку $\hat{u}(x^{2i}) = u(2i) = 0$, $i \geq 0$, в частности $\text{Ker } \hat{u}$ содержит многочлен 1.

Бипоследовательностью над модулем M назовем произвольную функцию

$$u: \mathbf{Z} \rightarrow M.$$

Множество всех бипоследовательностей над M обозначим $M_{\text{bi}}^{(1)}$. Бипоследовательность u будем называть линейной рекуррентной бипоследовательностью (ЛРБ) порядка m над модулем M , если существуют элементы $c_0, \dots, c_{m-1} \in R$ такие, что c_0 — обратимый элемент кольца R и условие (1) выполняется для всех $i \in \mathbf{Z}$. Многочлен

$$F(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0 \in R[x]$$

будем называть характеристическим многочленом ЛРБ u . Этот многочлен реверсивен. Вектор $u(0, m-1) = (u(0), \dots, u(m-1)) \in R^m$ назовем начальным вектором ЛРБ u . Последний термин предполагает, что вся ЛРБ u однозначно определяется своим начальным вектором, а это обеспечивается условием, что элемент c_0 обратим. Множество всех ЛРБ над M с характеристическим многочленом $F(x)$ обозначим через $L_M^{\text{bi}}(F)$, а множество всех ЛРБ над M — через $\mathcal{LM}_{\text{bi}}^{(1)}$.

Реверсом бипоследовательности u назовем бипоследовательность $u^*: \mathbf{Z} \rightarrow M$, определяемую равенствами

$$u^*(i) = u(-i), \quad i \in \mathbf{Z}.$$

Если $u \in L_M^{\text{bi}}(F)$, то $u^* \in L_M^{\text{bi}}(F^*)$, где $F^*(x) = x^m F(0)^{-1} F(1/x)$ — многочлен, сопряженный к $F(x)$, $m = \deg F(x)$. Пусть теперь $u \in L_M(F)$ — ЛРП с реверсивным характеристическим многочленом $F(x)$. Тогда u можно единственным образом продолжить до бипоследовательности $u \in L_M^{\text{bi}}(F)$ так, чтобы соотношение (1) выполнялось для всех $i \in \mathbb{Z}$. Реверсом реверсивной ЛРП u назовем ЛРП $u^*: \mathbb{N}_0 \rightarrow M$ со знаками $u^*(i) = u(-i)$, $i \geq 0$. Тогда $u^* \in L_M(F^*)$. По-другому реверс ЛРП можно определить следующим образом. Пусть v — ЛРП с характеристическим многочленом $F^*(x)$ и начальным вектором $v(0, m-1) = (u(m-1), \dots, u(0))$; тогда $u^* = x^{m-1}v$.

Каждой реверсивной ЛРП $u: \mathbb{N}_0 \rightarrow M$ можно сопоставить получающуюся из нее ЛРБ $u: \mathbb{Z} \rightarrow M$. Наоборот, если u — некоторая ЛРБ, то ее ограничение на $\mathbb{N}_0$ является реверсивной ЛРП. Рассматривая эти взаимно обратные биективные соответствия как отождествления, получим, что

$$\mathcal{L}M_{\text{bi}}^{(1)} \equiv \mathcal{L}M_{\text{rev}}^{(1)}. \quad (16)$$

Пусть $x^s u$ — сдвиг бипоследовательности u на s шагов влево:

$$(x^s u)(i) = u(i+s), \quad i \in \mathbb{Z}.$$

На абелевой группе $(M_{\text{bi}}^{(1)}, +)$ зададим структуру левого $R[x, x^{-1}]$ -модуля, определив умножение многочлена

$$F(x) = \sum_{s=-m}^n c_s x^s \in R[x, x^{-1}]$$

на бипоследовательность u правилом (12). Отметим, что ввиду (16) это определение индуцирует структуру $R[x, x^{-1}]$ -модуля также на множестве $\mathcal{L}M_{\text{rev}}^{(1)}$ реверсивных ЛРП, при котором $x^{-s}u$ есть сдвиг ЛРП u на s шагов вправо.

Идеал кольца $R[x, x^{-1}]$ назовем унитарным, если он содержит унитарный реверсивный многочлен из $R[x]$. Идеал

$$\text{An}(u) = \{F(x) \in R[x, x^{-1}]: F(x)u = 0\} \triangleleft R[x, x^{-1}]$$

назовем аннулятором бипоследовательности u . Очевидно, u есть ЛРБ над M тогда и только тогда, когда идеал $\text{An}(u)$ унитарен. При этом $u \in L_M^{\text{bi}}(F)$ тогда и только тогда, когда $F(x)u = 0$.

Отображение $\hat{u} \in R[x, x^{-1}]^* = \text{Hom}(R[x, x^{-1}], R)$ однозначно определяется своими значениями $\hat{u}(x^i)$, $i \in \mathbb{Z}$, и может быть отождествлено с бипоследовательностью $u \in R_{\text{bi}}^{(1)}$ со знаками $u(i) = \hat{u}(x^i)$, $i \in \mathbb{Z}$. Таким образом,

$$R[x, x^{-1}]^* \equiv R_{\text{bi}}^{(k)}. \quad (17)$$

Справедливы импликации

$$F(x) \in \text{An}(u) \iff F(x)R[x, x^{-1}] \subseteq \text{Ker } \hat{u}.$$

Следующее утверждение показывает, что при отождествлениях (13) и (17) множества $R[x]^\circ$ и $R[x, x^{-1}]^\circ$ совпадают с множествами $\mathcal{L}R^{(1)}$ и $\mathcal{L}R_{\text{bi}}^{(1)}$ всех ЛРП и ЛРБ над кольцом R соответственно.

Предложение 1. Пусть A — алгебра многочленов $R[x]$ или $R[x, x^{-1}]$ над коммутативным кольцом R с единицей, K — R -подмодуль в A . Тогда следующие утверждения эквивалентны:

- (a) $\exists I \subseteq K, I \triangleleft A, A/I$ — конечно порожденный свободный R -модуль.
 (b) $\exists I \subseteq K, I \triangleleft A, A/I$ — конечно порожденный проективный R -модуль.
 (c) $\exists I \subseteq K, I \triangleleft A, A/I$ — конечно порожденный R -модуль.
 (d) $\exists I \subseteq K, I \triangleleft A, I$ унитарен.

Доказательство. Импликации (a) $\Rightarrow$ (b) $\Rightarrow$ (c) очевидны. Пусть $A = R[x]$. Импликация (c) $\Rightarrow$ (d) доказана, например, в [23] (см. утверждение 10.1). А именно, пусть R -модуль $R[x]/I$ порождается элементами $F_1 + I, \dots, F_r + I$, и пусть m — максимальная из степеней многочленов $F_1, \dots, F_r$. Тогда R -модуль $R[x]/I$ порождается элементами $1 + I, x + I, \dots, x^m + I$. Следовательно,

$$x^{m+1} - \sum_{i=0}^m c_i x^i \in I$$

для некоторых $c_i \in R$, то есть выполнено условие (d). Импликация (d) $\Rightarrow$ (a) очевидна.

Пусть теперь $A = R[x, x^{-1}]$. Докажем, что (c) $\Rightarrow$ (d).

Из (c) следует, что R -модуль $R[x, x^{-1}]/I$ порождается конечным числом элементов $x^{-m} + I, x^{-m+1} + I, \dots, x^m + I$. Следовательно,

$$x^{-m-1} + x^{m+1} - \sum_{i=-m}^m c_i x^i \in I$$

для некоторых $c_i \in R$. Так как I — идеал, многочлен

$$F(x) = 1 + x^{2m+2} - \sum_{i=-m}^m c_i x^{i+m+1},$$

являющийся унитарным и реверсивным, принадлежит I . При этом

$$F(x)R[x, x^{-1}] \subseteq I \subseteq K.$$

Докажем, что (d) $\Rightarrow$ (a).

Пусть K содержит идеал $I = F(x)R[x, x^{-1}]$, где $F(x) \in R[x]$ — унитарный реверсивный многочлен степени m . Докажем, что $R[x, x^{-1}]/I$ — конечно порожденный свободный R -модуль с базисом $1 + I, x + I, \dots, x^{m-1} + I$. Очевидно, перечисленные элементы порождают R -модуль $R[x, x^{-1}]/I$, поэтому достаточно доказать их линейную независимость над R . Предположим противное. Тогда некоторый ненулевой элемент $F(x)G(x)$, $G(x) \in R[x, x^{-1}]$, идеала I имеет вид

$$\sum_{i=0}^{m-1} r_i x^i \in I, \quad r_i \in R, \quad i = 0, 1, \dots, m-1.$$

Введем обозначения

$$F(x) = \sum_{i=0}^m f_i x^i, \quad G(x) = \sum_{i=n}^N g_i x^i, \quad H(x) = F(x)G(x),$$

где $g_n \neq 0$, $g_N \neq 0$, $n \leq N$. Так как $F(x)$ унитарен, старший член $H(x)$ есть $g_N x^{m+N} \neq 0$. Так как $F(x)$ реверсивен, младший член $H(x)$ равен $f_0 g_n x^n \neq 0$. Чтобы произведение $F(x)G(x)$ имело указанный вид, необходимо, чтобы выполнялись условия $m + N < m$ и $n \geq 0$, что невозможно.

Следствие 1. *Справедливы равенства*

$$R[x]^* \equiv R^{(1)}, \quad R[x]^\circ \equiv \mathcal{L}R^{(1)}, \quad R[x, x^{-1}]^* \equiv R_{bi}^{(1)}, \quad R[x, x^{-1}]^\circ \equiv \mathcal{L}R_{bi}^{(1)} \equiv \mathcal{L}R_{rev}^{(1)}.$$

Доказательство. Докажем, например, последнее соотношение. Отображение $\hat{u} \in R[x, x^{-1}]^*$ принадлежит $R[x, x^{-1}]^\circ$ тогда и только тогда, когда $\text{Ker } \hat{u}$ содержит идеал $I \triangleleft R[x, x^{-1}]$ такой, что $R[x, x^{-1}]/I$ — конечно порожденный проективный R -модуль. Это равносильно тому, что $\text{Ker } \hat{u} \supseteq F(x)R[x, x^{-1}]$, где $F(x)$ — унитарный реверсивный многочлен, а это эквивалентно тому, что $u \in \mathcal{L}R_{bi}^{(1)}$.

4. Алгебры Хопфа линейных рекуррентных последовательностей

Пусть $R[x]^\bullet$ — биалгебра и $R[x]$, $R[x, x^{-1}]^\bullet$ — алгебры Хопфа многочленов, определенные в примере 1 и имеющие следующие операции:

$$\begin{aligned} (R[x], \cdot, 1, \Delta_x, \varepsilon_x, S_x), \\ (R[x]^\bullet, \cdot, 1, \Delta_x^\bullet, \varepsilon_x^\bullet), \\ (R[x, x^{-1}]^\bullet, \cdot, 1, \Delta_x^\bullet, \varepsilon_x^\bullet, S_x^\bullet). \end{aligned} \quad (18)$$

Так как $\Delta_x(x) = x \otimes 1 + 1 \otimes x$ и $\Delta_x^\bullet(x) = x \otimes x$, то

$$\begin{aligned} \Delta_x(x^i) &= (\Delta_x(x))^i = \sum_{j=0}^i \binom{i}{j} x^j \otimes x^{i-j}, \quad i \in \mathbb{N}_0, \\ \Delta_x^\bullet(x^i) &= x^i \otimes x^i, \quad i \in \mathbb{Z}. \end{aligned} \quad (19)$$

Введем обозначения для операций дуальных биалгебры и алгебр Хопфа:

$$\begin{aligned} (R[x]^\circ, *, e_*, \Delta, \varepsilon, S) &\equiv \mathcal{L}R^{(1)}, \\ (R[x]^{*\circ}, \cdot, e^\circ, \Delta, \varepsilon) &\equiv \mathcal{L}R^{(1)\bullet}, \\ (R[x, x^{-1}]^{*\circ}, \cdot, e^\circ, \Delta, \varepsilon, S^\circ) &\equiv \mathcal{L}R_{bi}^{(1)\bullet} \equiv \mathcal{L}R_{rev}^{(1)\bullet}. \end{aligned} \quad (20)$$

Здесь одинаковые символы обозначают одинаковые операции, возможно, определенные на разных множествах. В частности, поскольку структуры алгебр в биалгебрах (18) одинаковы, структуры коалгебр (коумножение Δ и коединица ε) во всех дуальных биалгебрах (20) одинаковы. При необходимости умножение в $R[x]^\circ$ будем обозначать через m_* , а умножение в $R[x]^{*\circ}$ — через m° . Эти операции будем называть конволюцией и покомножителем произведением последовательностей соответственно. Операции первых двух

биалгебр из (20) имеют следующие области определения и значений (для последней алгебры Хопфа в (20) соотношения аналогичны):

$$\begin{aligned}
 * &= m_*: \mathcal{LR}^{(1)} \otimes \mathcal{LR}^{(1)} \rightarrow \mathcal{LR}^{(1)} \text{ — конволюция последовательностей,} \\
 \cdot &= m^\bullet: \mathcal{LR}^{(1)} \otimes \mathcal{LR}^{(1)} \rightarrow \mathcal{LR}^{(1)} \text{ — покоординатное произведение,} \\
 e_*, e^\bullet &: R \rightarrow \mathcal{LR}^{(1)} \text{ — единицы относительно } * \text{ и } \cdot, \\
 \Delta &: \mathcal{LR}^{(1)} \rightarrow \mathcal{LR}^{(1)} \otimes \mathcal{LR}^{(1)} \text{ — коумножение,} \\
 \varepsilon &: \mathcal{LR}^{(1)} \rightarrow R \text{ — коединица,} \\
 S &: \mathcal{LR}^{(1)} \rightarrow \mathcal{LR}^{(1)} \text{ — антипод.}
 \end{aligned}$$

Пользуясь общими определениям (5), (6), (10), (11) и равенствами (19), запишем эти операции в явном виде. Пусть $\hat{u}, \hat{v}$ — функции из $R[x]^\circ$ или $R[x, x^{-1}]^\circ$ и u, v — соответствующие последовательности из $\mathcal{LR}^{(1)}$ или бипоследовательности из $\mathcal{LR}_{bi}^{(1)}$. Тогда в терминах функций операции дуальных алгебр задаются равенствами

$$\begin{aligned}
 (\hat{u} * \hat{v})(x^i) &= \sum_{j=0}^i \binom{i}{j} \hat{u}(x^j) \hat{v}(x^{i-j}), \\
 (\hat{u} \hat{v})(x^i) &= \hat{u}(x^i) \hat{v}(x^i), \\
 e_*(1)(x^i) &= \varepsilon_x(x^i) = (x^i)(0) = \delta_{i0}, \\
 e^\bullet(1)(x^i) &= \varepsilon_x^*(x^i) = (x^i)(1) = 1, \\
 \varepsilon(\hat{u}) &= \hat{u}(1) = \hat{u}(x^0), \\
 S(\hat{u})(x^i) &= \hat{u}(S_x(x^i)) = \hat{u}((-x)^i) = (-1)^i \hat{u}(x^i), \\
 S^\bullet(\hat{u})(x^i) &= \hat{u}(S_x^*(x^i)) = \hat{u}(x^{-i}).
 \end{aligned} \tag{21}$$

В терминах последовательностей эти равенства имеют вид

$$\begin{aligned}
 (u * v)(i) &= \sum_{j=0}^i \binom{i}{j} u(j) v(i-j), & (uv)(i) &= u(i) v(i), \\
 e_* &= (1, 0, 0, 0, \dots), & e^\bullet &= (1, 1, 1, 1, \dots), & \varepsilon(u) &= u(0), \\
 S(u)(i) &= (-1)^i u(i), & S^\bullet(u)(i) &= u(-i).
 \end{aligned} \tag{22}$$

Остается в явном виде определить коумножение Δ . Согласно (8)

$$\Delta \hat{u} = \sum_u \hat{u}_{(1)} \otimes \hat{u}_{(2)} \iff \forall i, j \quad \sum_u \hat{u}_{(1)}(x^i) \hat{u}_{(2)}(x^j) = \hat{u}(x^{i+j}),$$

или в терминах последовательностей

$$\Delta u = \sum_u u_{(1)} \otimes u_{(2)} \iff \forall i, j \quad \sum_u u_{(1)}(i) u_{(2)}(j) = u(i+j). \tag{23}$$

Для унитарного многочлена $F(x) \in R[x]$ степени m обозначим $e_t^F, 0 \leq t \leq m-1$, ЛРП из $L_R(F)$ с начальным вектором $e_t^F(0, m-1) = (0, \dots, 0, 1, 0, \dots, 0)$, где перед единицей находится t нулей. ЛРП $e^F = e_{m-1}^F$ называется импульсной последовательностью ЛРП-семейства $L_R(F)$. Если $F(x)$ реверсивен, то аналогично определяются ЛРБ $e_t^F \in L_R^{bi}(F)$, $0 \leq t \leq m-1$.

Предложение 2. Пусть u — (би)последовательность с (реверсивным) характеристическим многочленом $F(x)$ степени m . Тогда

$$\Delta u = \sum_{t=0}^{m-1} e_t^F \otimes x^t u.$$

Доказательство. Проверим справедливость правой части эквивалентности (23). Очевидно, если v — (би)последовательность с характеристическим многочленом $F(x)$, то $\sum_t e_t^F v(t) = v$. Отсюда,

$$\sum_{t=0}^{m-1} e_t^F(i)(x^t u)(j) = \left(\sum_{t=0}^{m-1} e_t^F(x^j u)(t) \right)(i) = (x^j u)(i) = u(i+j), \quad (24)$$

что и требовалось доказать.

Следствие 2. Если $F(x)$ и $G(x)$ — характеристические многочлены (би)последовательности u степеней m и n соответственно, то в модуле $R[x]^\circ \otimes R[x]^\circ$ выполняется равенство

$$\sum_{t=0}^{m-1} e_t^F \otimes x^t u = \sum_{s=0}^{n-1} e_s^G \otimes x^s u.$$

Следствие 3. ЛРП-семейства $L_R(F)$ и $L_R^{\text{bi}}(F)$ являются подкоалгебрами в $\mathcal{L}R^{(1)}$ и $\mathcal{L}R_{\text{bi}}^{(1)}$ соответственно.

Операции коумножения последовательности можно дать следующую интерпретацию. Произвольное отображение $v: \mathbb{N}_0^2 \rightarrow R$ назовем 2-последовательностью над кольцом R . 2-последовательность v можно также рассматривать как отображение $\hat{v} \in R[x_1, x_2]^* = \text{Hom}(R[x_1, x_2], R)$. Тогда для произвольной ЛРП $u \in R[x]^\circ$

$$\Delta u \in R[x]^\circ \otimes R[x]^\circ \equiv (R[x] \otimes R[x])^\circ \equiv R[x_1, x_2]^\circ \subseteq R[x_1, x_2]^*.$$

Следовательно, Δu можно рассматривать как 2-последовательность. Ее знаки определяются соотношением (9):

$$\Delta \hat{u}(x^i \otimes x^j) \equiv \Delta \hat{u}(x_1^i x_2^j) \equiv \hat{u}(x^{i+j}),$$

или в терминах последовательностей

$$\Delta u(i \otimes j) \equiv \Delta u(i, j) \equiv u(i+j).$$

Таким образом, Δu есть не что иное, как ганкелева матрица (бесконечных размеров) ЛРП u .

Подводя итог, сформулируем следующий результат.

Теорема 1. Пусть R — коммутативное кольцо с единицей.

(а) Алгебра Хопфа, дуальная к алгебре многочленов $R[x]$, есть алгебра $R[x]^\circ \equiv \mathcal{L}R^{(1)}$ всех ЛРП над кольцом R с операцией конволюции в качестве умножения последовательностей.

- (b) Биалгебра, дуальная к биалгебре многочленов $R[x]^\bullet$, есть биалгебра $R[x]^{\bullet\bullet} \equiv \mathcal{L}R^{(1)\bullet}$ всех ЛРП над кольцом R с операцией покомпонентного произведения в качестве умножения последовательностей.
- (c) Алгебра Хопфа, дуальная к алгебре $R[x, x^{-1}]^\bullet$ лорановских многочленов, есть алгебра $R[x, x^{-1}]^{\bullet\bullet} \equiv \mathcal{L}R_{bi}^{(1)\bullet}$ всех ЛРБ над кольцом R с операцией покомпонентного произведения в качестве умножения бипоследовательностей. Эта алгебра изоморфна алгебре Хопфа $\mathcal{L}R_{rev}^{(1)\bullet}$ всех реверсивных ЛРП над кольцом R , являющейся подалгеброй Хопфа в биалгебре $\mathcal{L}R^{(1)\bullet}$.

Отметим, что множество $\mathcal{L}R_{rev}^{(1)}$ реверсивных последовательностей не образует подалгебру в алгебре $\mathcal{L}R^{(1)}$, поскольку конволюция двух реверсивных последовательностей $u = (1, -1, 1, -1, \dots)$ и $v = (1, 1, 1, 1, \dots)$ равна $u * v = (1, 0, 0, 0, \dots)$ и не является реверсивной последовательностью.

Изучим действие структуры левого $R[x]$ -модуля на рассматриваемых алгебрах.

Биалгебра A° , дуальная к произвольной биалгебре A , является (A, A) -бимодулем относительно следующего внешнего умножения элемента $u \in A^\circ$ на элементы $a, b \in A$:

$$a \cdot u \cdot b \in A^\circ, \quad (a \cdot u \cdot b)(c) = u(bca), \quad c \in A. \quad (25)$$

Если A коммутативна, то достаточно рассматривать структуру левого A -модуля, при этом $a \cdot u = u\hat{a}$, где $\hat{a}: A \rightarrow A$ — гомотетия. В рассматриваемых случаях $A = R[x]$ или $A = R[x, x^{-1}]$ с учетом (14) получаем, что

$$F(x) \cdot u = u\hat{F} = F(x)u.$$

Таким образом, внешнее умножение, определяемое на биалгебрах (20) формулой (25), совпадает со структурами $R[x]$ - и $R[x, x^{-1}]$ -модулей из раздела 3.

Любая подкоалгебра $C \subseteq A^\circ$ является A -подмодулем в A° . Действительно, если $u \in C$, то $\Delta u = \sum_i u_{(1)} \otimes u_{(2)}$, где $u_{(1)}, u_{(2)} \in C$, и ввиду (8) для любых $a, b \in A$

$$u(ab) = \sum_i u_{(1)}(a)u_{(2)}(b).$$

Последнее равенство можно записать в виде

$$a \cdot u = \sum_i u_{(1)}(a)u_{(2)},$$

откуда следует, что $a \cdot u \in C$, то есть, что C является A -подмодулем в A° . В нашем случае получаем, что любая подкоалгебра $C \subseteq R[x]^\circ$ (или $C \subseteq R[x, x^{-1}]^\circ$) является $R[x]$ -подмодулем (или $R[x, x^{-1}]$ -подмодулем). Сформулированное выше следствие 3 можно рассматривать как частичное обращение этого свойства. Отметим, что если R — поле, то C является подкоалгеброй в $R[x]^\circ$ тогда и только тогда, когда C является $R[x]$ -подмодулем (см. [5]), но в общем случае это неверно. Например, если $R = \mathbb{Z}_4$, $u = (2, 2, 2, \dots) \in L_R(x-1)$, $C = R[x]u = \{0, u\}$, то C является $R[x]$ -подмодулем в $R[x]^\circ$, но не подкоалгеброй, поскольку $\Delta u = e^{x-1} \otimes u \notin C \otimes C = 0$.

Отображение $m: C \otimes A \rightarrow A$, $m(c \otimes a) = c \cdot a$, называется слабым (левым) действием коалгебры (C, Δ, ε) в алгебре $(A, *, 1)$, если для любых $a, b \in A$ и для любого $c \in C$ такого, что $\Delta c = \sum_c c_{(1)} \otimes c_{(2)}$, выполняются равенства

$$c \cdot (a * b) = \sum_c (c_{(1)} \cdot a) * (c_{(2)} \cdot b), \quad c \cdot 1 = \varepsilon(c)1. \quad (26)$$

Если при этом C — биалгебра и отображение m задает на A структуру левого C -модуля, то есть

$$(cd) \cdot a = c \cdot (d \cdot a), \quad 1 \cdot a = a,$$

где $d, 1 \in C$, то m называется действием, а алгебра A называется (левой) C -модульной алгеброй. С помощью (4) можно проверить, что если A° — биалгебра, дуальная к A , то отображение $m: A \otimes A^\circ \rightarrow A^\circ$, $m(a \otimes u) = a \cdot u$, определенное в (25), является действием, задающим структуру левой A -модульной алгебры на A° . В частности, структуры $R[x]$ - и $R[x, x^{-1}]$ -модулей из раздела 3 на биалгебрах (20) являются действиями в указанном выше смысле.

Пусть c — примитивный (групповой) элемент биалгебры A . Полагая в (26) $a = u$, $b = v \in A^\circ$, получим, что

$$c \cdot (u * v) = (c \cdot u) * v + u * (c \cdot v) \quad (\text{соответственно} \quad c \cdot (u * v) = (c \cdot u) * (c \cdot v))$$

(здесь $*$ — умножение в A°). Таким образом, отображение $A^\circ \rightarrow A^\circ$, $u \rightarrow c \cdot u$, является дифференцированием (соответственно эндоморфизмом) алгебры A° . В биалгебрах многочленов, полагая $c = x$, получаем, что

$$x(u * v) = xu * v + u * xv, \quad x(uv) = (xu)(xv). \quad (27)$$

Эти равенства показывают, что умножение (би)последовательности на x (сдвиг влево) является дифференцированием алгебры $R[x]^\circ$ и эндоморфизмом R -алгебр $R[x]^\circ$ и $R[x, x^{-1}]^\circ$. Полагая в (26) $c = x^n$, получаем, что в алгебре $R[x]^\circ$ верна формула

$$x^n(u * v) = \sum_{k=0}^n \binom{n}{k} (x^k u) * (x^{n-k} v), \quad (28)$$

являющаяся не чем иным как формулой Лейбница для n -й производной произведения двух функций. Отметим, что соотношения (27) легко проверяются непосредственно, а соотношения (28) получаются из них индукцией по n .

Для вычисления i -го знака конволюции последовательностей u и v с помощью определения (22) требуется знать знаки $u(j)$, $v(j)$ при всех $j \in \{0, 1, \dots, i\}$. На самом деле, как показывает следующее утверждение, знаки последовательности $u * v$ можно вычислять рекуррентно, храня в памяти матрицу фиксированного размера $m \times n$. В предложении 3 мы будем считать, что нумерация строк и столбцов матриц начинается с нуля. Элементы матрицы M будем обозначать M_{ij} . Сопровождающую $m \times m$ матрицу унитарного многочлена

$$F(x) = x^m - \sum_{s=0}^{m-1} f_s x^s \in R[x]$$

обозначим $S(F)$, она имеет вид

$$S(F) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & f_0 \\ e & 0 & 0 & \dots & 0 & f_1 \\ 0 & e & 0 & \dots & 0 & f_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & e & f_{m-1} \end{pmatrix}.$$

Предложение 3. Пусть $u \in L_R(F)$, $v \in L_R(G)$, где $F(x)$, $G(x) \in R[x]$ — унитарные многочлены степеней m и n соответственно. Определим последовательность матриц $M^{(k)} = (M_{ij}^{(k)})$ размеров $m \times n$ над кольцом R , полагая

$$\begin{aligned} M_{ij}^{(0)} &= u(i)v(j), & 0 \leq i \leq m-1, \quad 0 \leq j \leq n-1, \\ M^{(k+1)} &= S(F)^T M^{(k)} + M^{(k)} S(G), \quad k \geq 0. \end{aligned}$$

Тогда $(u * v)(k) = M_{0,0}^{(k)}$ при всех $k \geq 0$.

Доказательство. Докажем индукцией по k , что

$$M_{ij}^{(k)} = ((x^i u) * (x^j v))(k), \quad 0 \leq i \leq m-1, \quad 0 \leq j \leq n-1.$$

При $k = 0$

$$M_{ij}^{(0)} = u(i)v(j) = ((x^i u) * (x^j v))(0).$$

Пусть сформулированное утверждение доказано при некотором $k \geq 0$. Введем обозначения $A = S(F)^T M^{(k)}$, $B = M^{(k)} S(G)$. Если $i \in \{0, 1, \dots, m-2\}$, то

$$A_{ij} = M_{i+1,j}^{(k)} = (x^{i+1} u * x^j v)(k).$$

Если же $i = m-1$, то

$$\begin{aligned} A_{ij} &= \sum_{s=0}^{m-1} f_s M_{sj}^{(k)} = \sum_{s=0}^{m-1} f_s (x^s u * x^j v)(k) \\ &= \left(\left(\sum_{s=0}^{m-1} f_s x^s u \right) * x^j v \right)(k) = (x^m u * x^j v)(k). \end{aligned}$$

Таким образом, $A_{ij} = (x^{i+1} u * x^j v)(k)$ при любом $i \in \{0, 1, \dots, m-1\}$. Аналогично, $B_{ij} = (x^i u * x^{j+1} v)(k)$. Теперь, ввиду (27),

$$\begin{aligned} M_{ij}^{(k+1)} &= A_{ij} + B_{ij} = (x^{i+1} u * x^j v + x^i u * x^{j+1} v)(k) \\ &= (x(x^i u * x^j v))(k) = (x^i u * x^j v)(k+1), \end{aligned}$$

что доказывает шаг индукции.

5. Линейные рекурренты как рациональные ряды и представляющие функции

Пусть $M[[x]]$ и $M[x]$ — R -модули формальных степенных рядов и многочленов над модулем M . Ряд $a(x) \in M[[x]]$ назовем рациональным, если $G(x)a(x) \in M[x]$ для некоторого многочлена $G(x) \in R[x]$ такого, что $G(0) = 1$. Поскольку многочлен $G(x) \in R[x]$ обратим в $R[[x]]$ тогда и только тогда, когда элемент $G(0)$ обратим в R , рациональные функции есть в точности функции, представляющиеся как частное двух многочленов (над M и над R). Каждой последовательности $u \in M^{(k)}$ сопоставим ряд

$$u(x) = \sum_{i \geq 0} u(i)x^i \in M[[x]],$$

называемый (обыкновенной) производящей функцией последовательности u . Множество рациональных производящих функций (рядов) над M обозначим $M_{\text{rat}}[[x]]$.

Пусть $u \in L_M(F)$, где $F(x) \in R[x]$ — унитарный многочлен степени m . Положим $G(x) = x^m F(1/x)$. Тогда $G(x)$ — многочлен степени m , $G(0) = 1$ и, как легко видеть, $G(x)u(x)$ — многочлен степени, меньшей m , то есть $u(x)$ — рациональный ряд. Обратно, пусть $u(x)$ — рациональный ряд, $G(x)u(x) = H(x) \in M[x]$, $\deg G(x) = m$, $G(0) = 1$. Тогда $u \in L_M(x^k F(x))$, где $F(x) = x^m G(1/x)$, $k = \max\{0, \deg H(x) - m + 1\}$. Таким образом, правило $u \rightarrow u(x)$ задает взаимно однозначные соответствия

$$M^{(1)} \equiv M[[x]], \quad \mathcal{L}M^{(1)} \equiv M_{\text{rat}}[[x]].$$

Аналогично каждой бипоследовательности u над модулем M сопоставим ряд

$$u(x) = \sum_{i \in \mathbb{Z}} u(i)x^i \in M[[x, x^{-1}]],$$

называемый (обыкновенной) производящей функцией бипоследовательности u . Ряд $a(x) \in M[[x, x^{-1}]]$ назовем рациональным, если существует унитарный реверсивный многочлен $G(x) \in R[x]$ такой, что $G(x)a(x) = 0$. Легко увидеть, что $u \in L_M^{\text{bi}}(F)$ тогда и только тогда, когда $F^*(x)u(x) = 0$, где $F^*(x)$ — многочлен, сопряженный к $F(x)$. Поэтому имеются взаимно однозначные соответствия

$$M_{\text{bi}}^{(1)} \equiv M[[x, x^{-1}]], \quad \mathcal{L}M_{\text{bi}}^{(1)} \equiv M_{\text{rat}}[[x, x^{-1}]].$$

При $M = R$ указанные соответствия индуцируют на множествах рациональных рядов над R структуры биалгебры и алгебр Хопфа:

$$\begin{aligned} (R_{\text{rat}}[[x]], *, e_*, \Delta, \varepsilon, S) &\equiv \mathcal{L}R^{(1)} \equiv R[x]^\circ, \\ (R_{\text{rat}}[[x]]^\bullet, \cdot, e^\bullet, \Delta, \varepsilon) &\equiv \mathcal{L}R^{(1)\bullet} \equiv R[x]^\bullet, \\ (R_{\text{rat}}[[x, x^{-1}]]^\bullet, \cdot, e^\bullet, \Delta, \varepsilon, S^\bullet) &\equiv \mathcal{L}R_{\text{bi}}^{(1)\bullet} \equiv \mathcal{L}R_{\text{rev}}^{(1)\bullet} \equiv R[x, x^{-1}]^\bullet. \end{aligned}$$

Операции здесь являются операциями (22), (23), (9), выраженными в терминах формальных степенных рядов: если

$$a(x) = \sum a_i x^i, \quad b(x) = \sum b_i x^i,$$

то

$$\begin{aligned} a(x) * b(x) &= \sum_{k \geq 0} \sum_{i=0}^k \binom{k}{i} a_i b_{k-i} x^k, & a(x) \cdot b(x) &= \sum_i a_i b_i x^i, \\ \Delta a &= \sum_{i,j} a_{i+j} x^i \otimes x^j, & e_* &= 1, \\ e^\bullet &= \sum_i x^i, & \varepsilon(a) &= a(0) = a_0, \\ S(a) &= a(-x), & S^\bullet(a) &= a(x^{-1}). \end{aligned} \tag{29}$$

Умножение в алгебре $R_{\text{rat}}[[x]]$ можно назвать конволюцией рядов, умножение рядов в алгебрах $R_{\text{rat}}[[x]]^\bullet$ и $R_{\text{rat}}[[x, x^{-1}]]^\bullet$ производится по координатам (по Адамару).

Рациональный ряд $a(x) \in M[[x]]$ назовем реверсивным, если существует унитарный реверсивный многочлен $G(x) \in M[x]$ такой, что $G(x)a(x) \in M[x]$. Множество реверсивных рациональных рядов над R образует подалгебру Хопфа $R_{\text{rat}}[[x]]_{\text{rev}}^\bullet$ в подбиалгебре $R_{\text{rat}}[[x]]^\bullet$, изоморфную $R_{\text{rat}}[[x, x^{-1}]]^\bullet$.

Пусть $F(x) \in R[x]$ — унитарный многочлен степени m , e^F — импульсная последовательность семейства $L_R(F)$. Тогда произвольная ЛРП $u \in L_M(F)$ однозначно представляется в виде линейной комбинации последовательностей $e^F, xe^F, \dots, x^{m-1}e^F$ с коэффициентами из M :

$$u = \varphi_0 e^F + \varphi_1 x e^F + \dots + \varphi_{m-1} x^{m-1} e^F = \Phi(x) e^F,$$

где

$$\Phi(x) = \sum_{s=0}^{m-1} \varphi_s x^s \in M[x].$$

Многочлен $\Phi(x)$ называется генератором ЛРП u относительно характеристического многочлена $F(x)$. Введем обозначения

$$\Phi^{(*)}(x) = \sum \varphi_s x^{m-s-1}, \quad F^{(*)}(x) = x^m F(1/x) = F(0)F^*(x).$$

Тогда $F^{(*)}(0) = 1$ и справедлива формула

$$F^{(*)}(x)u(x) = \Phi^{(*)}(x).$$

Действительно, легко увидеть, что $F^{(*)}(x)e^F(x) = x^{m-1}$ и $(x^s e^F)(x) = x^{-s} e^F(x)$, откуда

$$\begin{aligned} F^{(*)}(x)u(x) &= F^{(*)}(x) \left(\sum_s \varphi_s x^s e^F \right) (x) = F^{(*)}(x) \sum_s \varphi_s x^{-s} e^F(x) \\ &= \sum_s \varphi_s x^{m-1-s} = \Phi^{(*)}(x). \end{aligned}$$

Таким образом, производящая функция ЛРП $u \in L_M(F)$ имеет вид

$$u(x) = \frac{\Phi^{(*)}(x)}{F^{(*)}(x)}.$$

Отсюда получаем формулу, позволяющую вычислять генератор ЛРП u :

$$\Phi^{(*)}(x) = u(x)F^{(*)}(x).$$

Если $u(x)$ — рациональный ряд над M и $G(x)u(x) = H(x) \in M[x]$, где $G(0) = 1$, $\deg G(x) = m$, то смысл многочлена $H(x)$ можно теперь объяснить следующим образом: $H(x) = \Phi^{(*)}(x)$, где $\Phi(x)$ — генератор ЛРП u относительно характеристического многочлена $F(x) = x^{m+k}G(1/x)$, $k = \max\{0, \deg H(x) - m + 1\}$.

Пусть кольцо R содержит поле рациональных чисел (если R — поле, то это условие равносильно тому, что R — поле характеристики 0). Тогда каждой последовательности u над модулем M можно сопоставить экспоненциальную производящую функцию

$$U(x) = \sum_{i \geq 0} u(i) \frac{x^i}{i!} \in M[[x]].$$

Экспоненциальный ряд назовем рациональным, если соответствующая обыкновенная производящая функция рациональна. Множество рациональных экспоненциальных рядов обозначим $M_{\text{rat}}^{\text{exp}}[[x]]$. Взаимно однозначное соответствие

$$\mathcal{L}M^{(1)} \equiv M_{\text{rat}}^{\text{exp}}[[x]], \quad u \equiv U(x),$$

при $M = R$ индуцирует структуру алгебры Хопфа

$$(R_{\text{rat}}^{\text{exp}}[[x]], *, e_*, \Delta, \varepsilon, S) \equiv \mathcal{L}R^{(1)} \equiv R[x]^\circ$$

со следующими операциями: если

$$A(x) = \sum a_i \frac{x^i}{i!}, \quad B(x) = \sum b_i \frac{x^i}{i!},$$

то

$$A(x) * B(x) = \sum_{k \geq 0} \sum_{i=0}^k \binom{k}{i} a_i b_{k-i} \frac{x^k}{k!}, \quad \Delta A = \sum_{i,j \geq 0} a_{i+j} \frac{x^i}{i!} \otimes \frac{x^j}{j!},$$

а e_*, ε, S задаются так же, как в (29). На самом деле, умножение в алгебре $R_{\text{rat}}^{\text{exp}}[[x]]$ есть обычное произведение рядов (по Коши):

$$\begin{aligned} A(x) * B(x) &= \sum_{k \geq 0} \frac{x^k}{k!} \sum_{i=0}^k \binom{k}{i} a_i b_{k-i} = \sum_{k \geq 0} x^k \sum_{i+j=k} \frac{a_i}{i!} \frac{b_j}{j!} \\ &= \sum_{i \geq 0} a_i \frac{x^i}{i!} \sum_{j \geq 0} b_j \frac{x^j}{j!} = A(x)B(x). \end{aligned}$$

Структура левого $R[x]$ -модуля на множестве последовательностей индуцирует структуру левого $R[x]$ -модуля на алгебре экспоненциальных производящих функций. Соответствующую внешнюю операцию обозначим

$$\bullet: R[x] \otimes R_{\text{rat}}^{\text{exp}}[[x]] \rightarrow R_{\text{rat}}^{\text{exp}}[[x]].$$

Если $v = x u$ — сдвиг последовательности u , то соответствующие экспоненциальные производящие функции связаны соотношением

$$V(x) = \sum_{i \geq 0} v(i) \frac{x^i}{i!} = \sum_{i \geq 0} u(i+1) \frac{x^i}{i!} = U'(x),$$

где штрих обозначает взятие производной. Таким образом, внешнее умножение на x индуцирует дифференцирование ряда по переменной x . Справедлива формула

$$F(x) \bullet A(x) = F\left(\frac{d}{dx}\right) A(x).$$

В частности, семейство $L_R(F)$ всех ЛРП, удовлетворяющих линейному рекуррентному соотношению (1), можно рассматривать как модуль решений линейного дифференциального уравнения

$$U^{(n)}(x) = c_{m-1} U^{(n-1)}(x) + \dots + c_1 U'(x) + c_0 U(x), \quad (30)$$

а каждую ЛРП $u \in L_R(F)$ — как решение $U(x)$, удовлетворяющее начальным условиям $U^{(i)}(0) = u(i)$, $i \in \{0, 1, \dots, m-1\}$.

В алгебрах обыкновенных производящих функций внешнее умножение на x индуцирует эндоморфизм сдвига коэффициентов ряда: $x \bullet a(x) = \sum_{i \geq 0} a_{i+1}x^i$ в алгебре $R[x]^\bullet$ и $x \bullet a(x) = \sum_{i \in \mathbb{Z}} a_{i+1}x^i = x^{-1}a(x)$ в алгебре $R[x, x^{-1}]^\bullet$.

Покажем теперь, что понятие линейной рекуррентной последовательности над модулем является частным случаем понятия представляющей функции. Пусть $(G, \cdot)$ — коммутативная полугруппа, M — левый R -модуль и M^G — множество всех функций $u: G \rightarrow M$. Это множество образует алгебру над кольцом R с поточечными операциями сложения и умножения функций и умножения на скаляры из R :

$$(u+v)(g) = u(g) + v(g), \quad (uv)(g) = u(g)v(g), \quad (ru)(g) = ru(g), \quad g \in G,$$

где $u, v \in M^G$, $r \in R$. Определим действие группы G на множестве M^G правилом

$$(gu)(h) = u(gh),$$

где $g, h \in G$, $u \in M^G$. Тогда M^G превращается в модуль над полугрупповым кольцом $R[G]$. Функция $u \in M^G$ называется представляющей, если циклический модуль $R[G]u = {}_R(gu: g \in G)$ конечно порожден над R . Множество представляющих функций обозначим $\mathcal{R}(M^G)$.

Если $G = (\mathbb{N}_0, +)$ — полугруппа целых неотрицательных чисел или изоморфная ей полугруппа $G = (\{x^i: i \in \mathbb{N}_0\}, \cdot)$ мономов, то M^G есть не что иное как множество $M^{(1)}$ всех последовательностей над M , полугрупповая алгебра $R[G]$ совпадает с алгеброй многочленов $R[x]$, и структура $R[G]$ -модуля на M^G совпадает с введенной в (12) структурой $R[x]$ -модуля на $M^{(1)}$. При этом модуль $R[G]u = R[x]u$ называется модулем сдвигов последовательности u . Аналогично, если $G = (\mathbb{Z}, +)$ или $G = (\{x^i: i \in \mathbb{Z}\}, \cdot)$, то $M^G = M_{\text{bi}}^{(1)}$ и $R[G] = R[x, x^{-1}]$.

Предложение 4. *(Би)последовательность является представляющей функцией тогда и только тогда, когда она является линейной рекуррентной (би)последовательностью. Таким образом,*

$$M^{\mathbb{N}_0} = M^{(1)}, \quad M^{\mathbb{Z}} = M_{\text{bi}}^{(1)}, \quad \mathcal{R}(M^{\mathbb{N}_0}) = \mathcal{L}M^{(1)}, \quad \mathcal{R}(M^{\mathbb{Z}}) = \mathcal{L}M_{\text{bi}}^{(1)}.$$

Доказательство. По определению последовательность u является представляющей функцией тогда и только тогда, когда ее модуль сдвигов $R[x]u$ конечно порожден как R -модуль. Это равносильно тому, что $R[x]u = {}_R(u, xu, \dots, x^{m-1}u)$ для некоторого $m \geq 1$. В свою очередь это условие равносильно тому, что u — ЛРП порядка m . Для бипоследовательностей доказательство аналогично.

Таким образом, линейные рекуррентные (би)последовательности над модулем можно рассматривать как представляющие функции на полугруппах $(\mathbb{N}_0, +)$ и $(\mathbb{Z}, +)$. Многие понятия и результаты этой работы можно изложить для представляющих функций на произвольной полугруппе с единицей, однако, нашей целью является рассмотрение непосредственно алгебр линейных рекуррентных последовательностей.

6. Групповые и примитивные элементы, интегралы и разделенные степени в алгебрах ЛРП

Пусть A° — биалгебра, дуальная к биалгебре A . Ввиду (9) элемент $u \in A^\circ$ является групповым, $\Delta u = u \otimes u$, тогда и только тогда, когда $u(a)u(b) = u(ab)$, $a, b \in A$, то есть $u: A \rightarrow R$ — гомоморфизм алгебр. В случае $A = R[x]$ это условие имеет вид $\hat{u}(x^{i+j}) = \hat{u}(x^i)\hat{u}(x^j)$, или в терминах последовательностей

$$u(i+j) = u(i)u(j).$$

Таковыми соотношениями описываются геометрические прогрессии $u(i) = a^i$. Следовательно, групповые элементы биалгебр $R[x]^\circ$ и $R[x]^\circ$ — это все геометрические прогрессии со знаменателями $a \in R$, а групповые элементы биалгебр $R[x, x^{-1}]^\circ$ и $\mathcal{L}R_{\text{rev}}^{(1)\bullet}$ — это геометрические прогрессии, знаменатели которых являются обратимыми элементами кольца R .

Чтобы понять, как умножаются групповые элементы, мы используем (4). Пусть $u = (a^i)$, $v = (b^i)$ — две геометрические прогрессии. Тогда в алгебре $(R[x]^\circ, *, e_*)$

$$\begin{aligned} (\hat{u} * \hat{v})(x) &= m_R(\hat{u} \otimes \hat{v})\Delta_x(x) = m_R(\hat{u} \otimes \hat{v})(x \otimes 1 + 1 \otimes x) \\ &= \hat{u}(x)\hat{v}(1) + \hat{u}(1)\hat{v}(x) = a + b, \end{aligned}$$

а в алгебре $(R[x]^\circ, \cdot, e^\bullet)$

$$(\hat{u}\hat{v})(x) = m_R(\hat{u} \otimes \hat{v})\Delta_x^\bullet(x) = m_R(\hat{u} \otimes \hat{v})(x \otimes x) = \hat{u}(x)\hat{v}(x) = ab.$$

Таким образом, $(a^i) * (b^i) = ((a+b)^i)$, $(a^i)(b^i) = (ab)^i$. Следовательно,

$$\begin{aligned} (G(R[x]^\circ), *) &\cong (R, +), \\ (G(R[x]^\circ), \bullet) &\cong (R, \bullet), \\ (G(R[x, x^{-1}]^\circ), \cdot) &\cong (G(\mathcal{L}R_{\text{rev}}^{(1)\bullet}), \cdot) \cong (U(R), \cdot), \end{aligned}$$

где $U(R)$ — мультипликативная группа кольца R .

В качестве следствия получаем, что биалгебру $R[x]^\circ$ нельзя превратить в алгебру Хопфа, то есть на ней нельзя задать антипод. Действительно, в алгебре Хопфа множество групповых элементов образует группу относительно умножения, в то время как $G(R[x]^\circ) \cong (R, \bullet)$ — не группа. Например, $G(R[x]^\circ)$ содержит геометрическую прогрессию $u = (1, 0, 0, 0, \dots)$, не являющуюся обратимым элементом алгебры $R[x]^\circ$.

Ввиду (9) последовательность u является примитивным элементом биалгебры $R[x]^\circ$, то есть $\Delta u = u \otimes e_* + e_* \otimes u$, тогда и только тогда, когда

$$u(i)e_*(j) + e_*(i)u(j) = u(i+j).$$

Так как $e_* = (1, 0, 0, 0, \dots)$, отсюда получаем, что

$$P(R[x]^\circ) = \{u = (0, a, 0, 0, 0, \dots) \in R^{(1)} : a \in R\}.$$

(Би)последовательность u из $R[x]^\circ$, $R[x, x^{-1}]^\circ$ или $\mathcal{L}R_{\text{rev}}^{(1)\bullet}$ является примитивным элементом этих биалгебр тогда и только тогда, когда $u(i)e^\bullet(j) + e^\bullet(i)u(j) = u(i+j)$. Так как $e_* = (1, 1, 1, 1, \dots)$, последнее условие записывается в виде

$$u(i) + u(j) = u(i+j)$$

и означает, что u — арифметическая прогрессия $u(i) = ai$. Таким образом, примитивные элементы трех указанных биалгебр — это арифметические прогрессии.

Отметим, что условие $u(i + j) = u(i) + u(j)$ в терминах функций записывается в виде $\hat{u}(x^{i+j}) = \hat{u}(x^i) + \hat{u}(x^j)$ и означает, что примитивные элементы — это те отображения $\hat{u} \in \text{Hom}(A, R)$, где $A = R[x]$ или $R[x, x^{-1}]$, которые являются гомоморфизмами мультипликативной полугруппы $(A, \cdot)$ алгебры A в аддитивную группу $(R, +)$ кольца R .

Множество примитивных элементов любой биалгебры является подгруппой ее аддитивной группы. Из полученных описаний видно, что множества примитивных элементов в рассматриваемых биалгебрах ЛРП изоморфны $(R, +)$.

Элемент a биалгебры A называется интегралом, если $ab = a\varepsilon(b)$ для любого элемента $b \in A$. Покажем, что в каждой из рассматриваемых биалгебр ЛРП множество интегралов совпадает с множеством (би)последовательностей, кратных (над R) единичному элементу данной биалгебры.

Если u — интеграл биалгебры $R[x]^\circ$, то $u * v = \varepsilon(u)v = u(0)v$ для всех $v \in R[x]^\circ$. Взяв $v = e_*$, получим, что $u = u(0)e_*$, то есть u кратна e_* . Обратно, если $u = ae_*$, то $u * v = av = u(0)v = \varepsilon(u)v$, то есть u — интеграл.

Если u — интеграл в одной из трех других биалгебр, то $uv = \varepsilon(u)v = u(0)v$. При $v = e^\bullet$ получим, что $u = u(0)e^\bullet$, то есть u кратна $e^\bullet$. Обратно, если $u = ae^\bullet$, то $uv = av = u(0)v = \varepsilon(u)v$, то есть u — интеграл.

Биномиальной последовательностью над кольцом R с корнем $a \in R$ порядка $n \geq 0$ называется последовательность $a^{[n]} \in R^{(k)}$ со знаками

$$a^{[n]}(0, n) = (0, \dots, 0, 1), \quad a^{[n]}(i) = \binom{i}{n} a^{i-n}, \quad i > n.$$

Формулу $a^{[n]}(i) = \binom{i}{n} a^{i-n}$ будем использовать при всех $i \geq 0$, считая, что $a^0 = e$ для любого $a \in R$, и что если $\binom{i}{n} = 0$, то и $\binom{i}{n} a^{i-n} = 0$ независимо от того, определена ли степень a^{i-n} . Легко видеть, что биномиальная последовательность $a^{[n]}$ есть импульсная последовательность семейства $L_R((x-a)^{n+1})$. Биномиальная последовательность $a^{[n]}$ реверсивна тогда и только тогда, когда элемент a кольца R обратим. В этом случае последовательность $a^{[n]}$ можно продолжить до бипоследовательности $a^{[n]} \in L_R^{\text{bi}}((x-a)^{n+1})$, полагая

$$a^{[n]}(i) = \binom{i}{n} a^{i-n}, \quad i \in \mathbb{Z},$$

где

$$\binom{i}{n} = \frac{i(i-1)\dots(i-n+1)}{n!}, \quad n \geq 0.$$

Такую бипоследовательность $a^{[n]}$, где $a \in R$ обратим, $n \geq 0$, будем называть биномиальной бипоследовательностью.

Последовательность элементов $c_0, c_1, \dots$ коалгебры C называется последовательностью разделенных степеней, если

$$\Delta c_n = \sum_{k=0}^n c_k \otimes c_{n-k}, \quad n \geq 0.$$

Проверим, что биномиальные (би)последовательности $a^{[n]}$, $n \geq 0$, образуют последовательность разделенных степеней в биалгебрах $R[x]^\circ$ и $R[x]^\bullet$, а если элемент a обратим,

то в бигалгебрах $R[x, x^{-1}]^{\circ\circ}$ и $\mathcal{L}R_{\text{rev}}^{(1)\bullet}$. Ввиду (23) требуется проверить, что

$$\sum_{k=0}^n a^{[k]}(i) \otimes a^{[n-k]}(j) = a^{[n]}(i+j).$$

Действительно,

$$\sum_{k=0}^n \binom{i}{k} a^{i-k} \binom{j}{n-k} a^{j-n+k} = \sum_{k=0}^n \binom{i}{k} \binom{j}{n-k} a^{i+j-n} = \binom{i+j}{n} a^{i+j-n},$$

что и требовалось доказать.

Пусть многочлен $F(x) \in R[x]$ представляется в виде

$$F(x) = (x - a_1)^{m_1} \dots (x - a_t)^{m_t},$$

где $a_i - a_j \in U(R)$ при $1 \leq i < j \leq t$. Тогда многочлены $(x - a_1)^{m_1}, \dots, (x - a_t)^{m_t}$ попарно взаимно просты, R -модуль $L_R(F)$ раскладывается в прямую сумму

$$L_R(F) = L_R((x - a_1)^{m_1}) \dot{+} \dots \dot{+} L_R((x - a_t)^{m_t})$$

и является свободным R -модулем с базисом $\{a_s^{[n_s]}, 0 \leq n_s \leq m_s - 1, 1 \leq s \leq t\}$, состоящим из биномиальных последовательностей [17]. Если кольцо R содержит поле рациональных чисел, то экспоненциальная производящая функция $A(x)$ биномиальной последовательности $a^{[n]}$ имеет вид

$$A(x) = \sum_{i \geq 0} \binom{i}{n} a^{i-n} \frac{x^i}{i!} = \frac{x^n}{n!} \sum_{i \geq n} \frac{(ax)^{i-n}}{(i-n)!} = \frac{x^n}{n!} e^{ax}.$$

Таким образом, биномиальный базис в терминах экспоненциальных производящих функций есть стандартный базис

$$\frac{x^{n_s}}{n_s!} e^{a_s x}, \quad 0 \leq n_s \leq m_s - 1, \quad 1 \leq s \leq t,$$

модуля решений линейного дифференциального уравнения (30) с характеристическим многочленом $F(x)$.

Соотношение

$$a^{[n]}(i) = \binom{i}{n} a^{i-n}$$

в терминах функций из $\text{Hom}(R[x], R)$ записывается в виде

$$\hat{a}^{[n]}(x^i) = \binom{i}{n} a^{i-n} = \frac{(x^i)^{(n)}(a)}{n!},$$

где верхний индекс (n) означает n -ю производную. Следовательно,

$$\hat{a}^{[n]}(F(x)) = \frac{F^{(n)}(a)}{n!}$$

есть n -й коэффициент ряда Тейлора в точке a для многочлена $F(x)$. Формула Тейлора для многочлена $F(x)$ в точке $a \in R$ записывается в виде

$$F(x) = \sum_{n \geq 0} \hat{a}^{[n]}(F(x))(x - a)^n = \sum_{n \geq 0} (F(x)a^{[n]})(0)(x - a)^n,$$

причем такая формула Тейлора уже не требует предположения о том, что R содержит поле рациональных чисел. В терминах последовательностей это равенство записывается в виде $(F(x)a^{[n]})(0) = F^{(n)}(a)/n!$. В частности, $\hat{0}^{[n]}(0)$, $n \geq 0$, — это коэффициенты многочлена $F(x)$, в чем легко убедиться непосредственно.

7. Хопфов модуль линейных рекуррент над модулем

Выше были рассмотрены структуры биалгебр и алгебр Хопфа на множестве $\mathcal{LR}^{(k)}$ ЛРП над кольцом R . В этом параграфе мы покажем, что множество $\mathcal{LM}^{(1)}$ всех ЛРП над R -модулем M образует хопфов модуль над алгеброй $\mathcal{LR}^{(1)}$ всех ЛРП над кольцом R .

Модуль M над основным кольцом R называется левым C -комодулем над коалгеброй (C, Δ, ε) , если имеется структурное отображение $\rho: M \rightarrow C \otimes M$, удовлетворяющее условиям

$$(\Delta \otimes 1_M)\rho = (1_C \otimes \rho)\rho, \quad (\varepsilon \otimes 1_M)\rho \equiv 1_M, \quad (31)$$

где используется отождествление $R \otimes M \equiv M$. Всякая коалгебра C является левым C -комодулем относительно структурного отображения $\rho = \Delta$, при этом условия (31) превращаются в аксиомы коассоциативности и коунитарности. Действие структурного отображения записывается в виде

$$\rho(m) = \sum_m m_{(1)} \otimes m_{(2)}, \quad m_{(1)} \in C, \quad m, m_{(2)} \in M. \quad (32)$$

Модуль M называется левым хопфовым H -модулем над алгеброй Хопфа (или биалгеброй) H , если M является левым H -модулем, левым H -комодулем со структурным отображением $\rho: M \rightarrow H \otimes M$, причем для любых $m \in M$ и $h \in H$ при условии $\Delta h = \sum_h h_{(1)} \otimes h_{(2)}$ выполняется соотношение

$$\rho(hm) = \sum_{h,m} h_{(1)}m_{(1)} \otimes h_{(2)}m_{(2)}. \quad (33)$$

Поскольку множество $\mathcal{LM}^{(1)}$ ЛРП над модулем M является левым $R[x]$ -модулем, естественно попытаться задать структурное отображение $\rho: \mathcal{LM}^{(1)} \rightarrow R[x] \otimes \mathcal{LM}^{(1)}$ так, чтобы превратить $\mathcal{LM}^{(1)}$ в хопфов модуль над кольцом многочленов. В связи с этим отметим, что произвольный левый H -модуль M над биалгеброй H является левым H -комодулем относительно тривиального структурного отображения $\rho(m) = 1 \otimes m$. В частности, R -модули $\mathcal{LM}^{(1)}$, $\mathcal{LM}^{(1)}$, $\mathcal{LM}_{\text{bi}}^{(1)}$, $\mathcal{LM}_{\text{rev}}^{(1)}$ являются левыми соответственно $R[x]$ -, $R[x]^*$ -, $R[x, x^{-1}]^*$ - и $R[x]^*$ -модулями и комодулями относительно тривиального структурного отображения $\rho(u) = 1 \otimes u$. Эти левые модули и комодули не являются хопфовыми модулями, поскольку во всех случаях соотношение (33), которое принимает вид

$$\Delta F = \sum_F F_{(1)} \otimes F_{(2)} \implies \rho(F(x)u) = \sum_F F_{(1)}(x) \otimes F_{(2)}(x)u,$$

$\Delta \in \{\Delta_x, \Delta_x^\bullet\}$, не выполняется, например, при $F(x) = x$.

Определим конволюцию и покоординатное произведение последовательности z над кольцом R и последовательности u над модулем M как последовательности $z * u$ и zu над модулем M со знаками

$$(z * u)(i) = \sum_{k=0}^i \binom{i}{k} z(k)u(i-k), \quad (zu)(i) = z(i)u(i), \quad i \geq 0.$$

Эти операции задают структуры левого $\mathcal{LR}^{(1)}$ -модуля и левого $\mathcal{LR}^{(1)\bullet}$ -модуля на множестве $\mathcal{LM}^{(1)}$. Аналогично определяется покоординатное произведение бипоследовательностей над R и M и структура левого $\mathcal{LR}_{bi}^{(1)\bullet}$ -модуля на $\mathcal{LM}_{bi}^{(1)}$.

Зададим отображение $\rho: \mathcal{LM}^{(1)} \rightarrow \mathcal{LR}^{(1)} \otimes \mathcal{LM}^{(1)}$ следующим образом: если $u \in L_M(F)$, $\deg F(x) = m$, то

$$\rho(u) = \sum_{t=0}^{m-1} e_t^F \otimes x^t u. \quad (34)$$

Точно так же отображение $\rho: \mathcal{LM}_{bi}^{(1)} \rightarrow \mathcal{LR}_{bi}^{(1)} \otimes \mathcal{LM}_{bi}^{(1)}$ задается для бипоследовательностей.

Теорема 2. Модули $\mathcal{LM}^{(1)}$, $\mathcal{LM}^{(1)}$, $\mathcal{LM}_{bi}^{(1)}$, $\mathcal{LM}_{rev}^{(1)}$ являются левыми хопфовыми соответственно $\mathcal{LR}^{(1)}$ -, $\mathcal{LR}^{(1)\bullet}$ -, $\mathcal{LR}_{bi}^{(1)\bullet}$ -, $\mathcal{LR}_{rev}^{(1)\bullet}$ -модулями относительно структурного отображения (34).

Доказательство. Зафиксируем некоторую систему образующих $(m_\alpha, \alpha \in A)$ R -модуля M . Тогда произвольную ЛРП $u \in L_M(F)$ можно представить в виде

$$u = \sum_{\alpha \in A} u_\alpha m_\alpha, \quad (35)$$

где $u_\alpha \in L_R(F)$, $\alpha \in A$, и лишь конечное число последовательностей u_α не равны 0. Действительно, пусть $\deg F(x) = m$. Представим элементы $u(i) \in M$ в виде

$$u(i) = \sum_{\alpha} c_{i\alpha} m_\alpha, \quad 0 \leq i \leq m-1,$$

где лишь конечное число элементов $c_{i\alpha} \in R$ отличны от 0. Обозначим через u_α ЛРП из $L_R(F)$ с начальным вектором $(c_{0\alpha}, \dots, c_{m-1,\alpha})$, $\alpha \in A$. Тогда лишь конечное число $u_\alpha \neq 0$, и $\sum_{\alpha} u_\alpha m_\alpha$ — последовательность из $L_M(F)$, начальный вектор которой совпадает с $u(0, m-1)$. Следовательно, справедливо равенство (35). Если u реверсивна, то все u_α можно выбрать реверсивными. Представление (35) имеет место и для бипоследовательностей.

Докажем, что перечисленные в формулировке структуры левых модулей заданы корректно. Для этого покажем, что конволюция и покоординатное произведение ЛРП z над R и ЛРП u над M есть ЛРП над M . Справедливы соотношения

$$z * u = z * \sum_{\alpha \in A} u_\alpha m_\alpha = \sum_{\alpha \in A} (z * u_\alpha) m_\alpha, \quad zu = \sum_{\alpha \in A} (zu_\alpha) m_\alpha.$$

Так как в силу теоремы 1 конволюция и покоординатное произведение ЛРП z и u_α над кольцом R есть ЛРП над R (например, с характеристическим многочленом $F_\alpha(x)$), то конволюция и покоординатное произведение ЛРП z и u есть ЛРП над модулем M (характеристический многочлен которой равен произведению конечного числа многочленов $F_\alpha(x)$, $\alpha \in A$, таких, что $u_\alpha \neq 0$). Для реверсивных последовательностей и бипоследовательностей рассуждения аналогичны. Аксиомы модуля, в частности, ассоциативность $z_1 * (z_2 * u) = (z_1 * z_2) * u$ и $z_1(z_2 u) = (z_1 z_2)u$, проверяются непосредственно (либо с помощью представления (35)).

Докажем, что отображение ρ задано корректно, то есть не зависит от выбора характеристического многочлена $F(x)$ ЛРП u (или ЛРБ u). Пусть $G(x)$ — другой характеристический многочлен ЛРП u степени n . Тогда u можно представить в виде

$$u = \sum_{\alpha} v_{\alpha} m_{\alpha},$$

где $v_{\alpha} \in L_R(G)$ и лишь конечное число $v_{\alpha} \neq 0$. При этом $u_{\alpha}, v_{\alpha} \in L_R(FG)$. Пользуясь следствием 2 (то есть фактически корректностью определения коумножения Δ формулой из утверждения 2), получаем, что

$$\begin{aligned} \sum_{t=0}^{m-1} e_t^F \otimes x^t u &= \sum_{t=0}^{m-1} e_t^F \otimes x^t \sum_{\alpha} u_{\alpha} m_{\alpha} \\ &= \sum_{\alpha} \left(\sum_{t=0}^{m-1} e_t^F \otimes x^t u_{\alpha} \right) m_{\alpha} = \sum_{\alpha} \left(\sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t u_{\alpha} \right) m_{\alpha} \\ &= \sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t \sum_{\alpha} u_{\alpha} m_{\alpha} = \sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t u, \end{aligned}$$

и аналогично,

$$\sum_{t=0}^{n-1} e_t^G \otimes x^t u = \sum_{t=0}^{n+m-1} e_t^{GF} \otimes x^t u.$$

Тем самым показано, что отображение ρ задано корректно.

Докажем, что ρ является структурным отображением, то есть выполнены условия (31). Пусть $u \in L_M(F)$. Тогда

$$\begin{aligned} (\Delta \otimes 1)\rho(u) &= (\Delta \otimes 1) \sum_{t=0}^{m-1} e_t^F \otimes x^t u = \sum_{t=0}^{m-1} \sum_{s=0}^{m-1} e_s^F \otimes x^s e_t^F \otimes x^t u, \\ (1 \otimes \rho)\rho(u) &= (1 \otimes \rho) \sum_{s=0}^{m-1} e_s^F \otimes x^s u = \sum_{s=0}^{m-1} \sum_{t=0}^{m-1} e_s^F \otimes e_t^F \otimes x^{s+t} u. \end{aligned}$$

Чтобы доказать равенство, достаточно проверить, что для любого s , $0 \leq s \leq m-1$,

$$\sum_{t=0}^{m-1} x^s e_t^F \otimes x^t u = \sum_{t=0}^{m-1} e_t^F \otimes x^{s+t} u.$$

В силу изоморфизма $R[x]^\circ \otimes R[x]^\circ \equiv (R[x] \otimes R[x])^\circ$ достаточно убедиться в том, что для любых i, j

$$\sum_{t=0}^{m-1} (x^s e_t^F)(i)(x^t u)(j) = \sum_{t=0}^{m-1} (e_t^F)(i)(x^{s+t} u)(j).$$

Но обе части равны $u(i + j + s)$ (см. (24)). Проверим второе условие в (31):

$$(\varepsilon \otimes 1)\rho(u) = \sum_{t=0}^{m-1} \varepsilon(e_t^F) \otimes x^t u = \sum_{t=0}^{m-1} e_t^F(0) \otimes x^t u = 1 \otimes u \equiv u.$$

Остается проверить условие (33). Так как в этом условии задействовано умножение последовательностей, доказательства существенно различаются для конволюции и покомпонентного произведения последовательностей.

Пусть $z \in L_R(G)$, $u \in L_M(F)$, $z * u \in L_M(H)$. Тогда условие (33) принимает вид

$$\sum_r e_r^H \otimes x^r (z * u) = \sum_s \sum_t (e_s^G * e_t^F) \otimes (x^s z * x^t u).$$

Достаточно проверить, что для любых $i, j \geq 0$

$$\sum_r e_r^H(i) x^r (z * u)(j) = \sum_s \sum_t (e_s^G * e_t^F)(i)(x^s z * x^t u)(j).$$

Аналогично (24) проверяется, что левая часть равна $(z * u)(i + j)$. Преобразуем правую часть:

$$\begin{aligned} & \sum_s \sum_t \sum_k \binom{i}{k} e_s^G(k) e_t^F(i - k) \sum_l \binom{j}{l} z(s + l) u(t + j - l) \\ &= \sum_k \binom{i}{k} \sum_l \binom{j}{l} \sum_s e_s^G(k) z(s + l) \sum_t e_t^F(i - k) u(t + j - l) \\ &= \sum_k \binom{i}{k} \sum_l \binom{j}{l} z(k + l) u(i + j - k - l) \\ &= \sum_k \binom{i}{k} (x^k z * x^{i-k} u)(j) = x^i (z * u)(j) = (z * u)(i + j), \end{aligned}$$

где предпоследнее равенство следует из (28).

Проверим условие (33) в случае, когда последовательности умножаются покомпонентно. Пусть $z \in L_R(G)$, $u \in L_M(F)$, $zu \in L_M(H)$. Условие (33) принимает вид

$$\sum_r e_r^H \otimes x^r (zu) = \sum_s \sum_t (e_s^G e_t^F) \otimes (x^s z)(x^t u).$$

Достаточно проверить, что для любых $i, j \geq 0$

$$\sum_r e_r^H(i)(zu)(r + j) = \sum_s \sum_t e_s^G(i) e_t^F(i) z(s + j) u(t + j),$$

или

$$(zu)(i + j) = \sum_s e_s^G(i) z(s + j) \sum_t e_t^F(i) u(t + j),$$

или

$$(zu)(i + j) = z(i + j)u(i + j).$$

Таким образом, условие (33) выполняется. Для реверсивных последовательностей и би-последовательностей все доказательства сохраняются.

8. Обобщение на полилинейные рекуррентные последовательности

Произвольная функция $u: \mathbb{N}_0^k \rightarrow M$ называется k -последовательностью над R -модулем M . Любую k -последовательность можно рассматривать как бесконечный k -мерный массив, заполненный элементами модуля M . Множество всех k -последовательностей над M обозначим $M^{(k)}$.

Будем говорить, что k -последовательность u является k -линейной рекуррентной последовательностью (k -ЛРП) над модулем M , если существуют унитарные многочлены $F_1(x), \dots, F_k(x) \in R[x]$ такие, что для любого $s \in \{1, \dots, k\}$ и для любых $i_1, \dots, i_{s-1}, i_{s+1}, \dots, i_k \in \mathbb{N}_0$ последовательность $v(i) = u(i_1, \dots, i_{s-1}, i, i_{s+1}, \dots, i_k)$, $i \geq 0$, есть ЛРП над R -модулем M с характеристическим многочленом $F_s(x)$. В случае $k = 1$ определение 1-ЛРП совпадает с определением ЛРП. Многочлены $F_1(x_1), \dots, F_k(x_k)$ из кольца $R[x] = R[x_1, \dots, x_k]$ многочленов от k переменных называются элементарными характеристическими многочленами k -ЛРП u . Множество всех k -ЛРП над M обозначим $\mathcal{LM}^{(k)}$, а множество k -ЛРП с элементарными характеристическими многочленами $F_1(x_1), \dots, F_k(x_k)$ будем обозначать через $L_M(F) = L_M(F_1, \dots, F_k)$. Назовем k -ЛРП u реверсивной, если $u \in L_M(F)$, где каждый из многочленов $F_1(x), \dots, F_k(x)$ реверсивен. Множество реверсивных k -ЛРП над M обозначим $\mathcal{LM}_{\text{rev}}^{(k)}$.

Например, 2-последовательность, рассматриваемая как двумерный массив, принадлежит $L_M(F_1, F_2)$ тогда и только тогда, когда последовательность в каждой строке массива есть ЛРП над M с характеристическим многочленом $F_1(x)$, а последовательность в каждом столбце — ЛРП с характеристическим многочленом $F_2(x)$.

Для $x = (x_1, \dots, x_k)$ и $s = (s_1, \dots, s_k)$ введем обозначение $x^s = x_1^{s_1} \dots x_k^{s_k}$. Сдвигом k -последовательности $u \in M^{(k)}$ на вектор s называется k -последовательность $x^s u$ со знаками $x^s u(i) = u(s + i)$, $i \in \mathbb{N}_0^k$. Определим умножение многочлена $F(x) = \sum_s c_s x^s \in R[x]$ на k -последовательность u правилом

$$F(x)u = \sum_s c_s x^s u, \quad \text{то есть} \quad (F(x)u)(i) = \sum_s c_s u(i + s), \quad i \in \mathbb{N}_0^k. \quad (36)$$

Тогда $M^{(k)}$ превращается в левый $R[x]$ -модуль. Идеал

$$\text{An}(u) = \{F(x) \in R[x] : F(x)u = 0\}$$

назовем аннулятором k -последовательности u . Тогда u есть k -ЛРП над M в том и только в том случае, когда идеал $\text{An}(u)$ унитарен, то есть содержит набор унитарных многочленов $F_1(x_1), \dots, F_k(x_k)$.

Каждой k -последовательности $u \in \mathcal{LR}^{(k)}$ над кольцом R сопоставим отображение

$$\hat{u} \in R[x]^* = \text{Hom}(R[x], R), \quad \hat{u}(x^i) = u(i), \quad i \in \mathbb{N}_0^k.$$

Это сопоставление взаимно однозначно и индуцирует на $R[x]^*$ структуру левого $R[x]$ -модуля по правилу $F(x)\hat{u} = \hat{u}\hat{F}$, где $\hat{F}: R[x] \rightarrow R[x]$, $\hat{F}(G) = GF$, — гомотетия. При этом

$$F(x) \in \text{An}(u) \iff F(x)R[x] \subseteq \text{Ker } \hat{u}.$$

Произвольная функция $u: \mathbb{Z}^k \rightarrow M$ называется k -бипоследовательностью над M . Пусть $R[x, x^{-1}]$ — алгебра многочленов Лорана от k переменных из примера 2. Введем на множестве k -бипоследовательностей $M_{\text{bi}}^{(k)}$ структуру левого $R[x, x^{-1}]$ -модуля, определив умножение многочлена

$$F(x) = \sum_{s \in \mathbb{Z}^k} c_s x^s \in R[x, x^{-1}]$$

на k -бипоследовательность u правилом (36). Идеал

$$\text{An}(u) = \{F(x) \in R[x, x^{-1}]: F(x)u = 0\}$$

называется аннулятором k -бипоследовательности u .

Идеал кольца $R[x, x^{-1}]$ будем называть унитарным, если он содержит набор унитарных реверсивных многочленов $F_1(x_1), \dots, F_k(x_k)$ из $R[x]$. Эти многочлены назовем элементарными характеристическими многочленами. Назовем u k -линейной рекуррентной бипоследовательностью (k -ЛРБ), если $\text{An}(u)$ — унитарный идеал. Множество всех k -ЛРБ с элементарными характеристическими многочленами $F_1(x_1), \dots, F_k(x_k)$ обозначим $L_M^{\text{bi}}(F) = L_M^{\text{bi}}(F_1, \dots, F_k)$.

Если $u \in L_M(F_1, \dots, F_k)$, $\deg F_s = m_s$, $\mathbf{m} = (m_1, \dots, m_s)$, то множество

$$\Pi = \Pi(\mathbf{m}) = \{0, 1, \dots, m_1 - 1\} \times \dots \times \{0, 1, \dots, m_k - 1\}$$

называется начальным параллелепипедом k -ЛРП u . Пусть $\Pi = \{i_1, \dots, i_m\}$, где $m = |\Pi| = m_1 \dots m_k$. Тогда вектор $u[\Pi] = (u(i_1), \dots, u(i_m)) \in M^\Pi = M^m$ назовем начальным вектором k -ЛРП u . Для каждого $\delta[\Pi] \in M^\Pi$ существует единственная k -ЛРП $u \in L_M(F)$ с начальным вектором $u[\Pi] = \delta[\Pi]$. Действительно, например, в случае $k = 2$ для получения u продолжим $\delta[\Pi]$ до m_2 последовательностей $u(i, j)$, $i \geq 0$, $0 \leq j < m_2$, из $L_M(F_1)$ и расположим их в первых m_2 строках бесконечного массива, а затем каждый начальный вектор $u(i, j)$, $0 \leq j < m_2$, продолжим до последовательности $u(i, j)$, $j \geq 0$, расположенной в i -м столбце массива, $i \geq 0$. Из сказанного следует, что $L_M(F)$ есть свободный R -модуль ранга m . Аналогичное утверждение верно для бипоследовательностей из $L_M^{\text{bi}}(F)$. Для $t \in \Pi$ через e_t^F будем обозначать k -(би)последовательность из $L_R(F)$ или $L_R^{\text{bi}}(F)$ с начальным вектором $e_t^F(t) = 1$, $e_t^F(i) = 0$ при $i \in \Pi(\mathbf{m}) \setminus \{t\}$. (Би)последовательность $e^F = e_{m-1}^F$ назовем импульсной (би)последовательностью семейств $L_R(F)$ и $L_R^{\text{bi}}(F)$. Реверсом k -бипоследовательности u назовем k -бипоследовательность $u^*: \mathbb{Z}^k \rightarrow M$, определяемую равенствами $u^*(i) = u(-i)$, $i \in \mathbb{Z}^k$. Каждую реверсивную k -ЛРП $u \in L_M(F)$ можно единственным образом продолжить до k -ЛРБ $u \in L_M^{\text{bi}}(F)$ с тем же начальным вектором $u[\Pi]$. Отождествляя реверсивную k -ЛРП и указанную k -ЛРБ, получим, что

$$\mathcal{L}M_{\text{rev}}^{(k)} \equiv \mathcal{L}M_{\text{bi}}^{(k)}.$$

Реверсом реверсивной k -ЛРП u назовем k -ЛРП u^* со знаками $u^*(i) = u(-i)$, $i \in \mathbb{N}_0^k$.

Каждой k -бипоследовательности $u \in M_{\text{bi}}^{(k)}$ сопоставим отображение

$$\hat{u} \in R[x, x^{-1}]^* = \text{Hom}(R[x, x^{-1}], R), \quad \hat{u}(x^i) = u(i), \quad i \in \mathbb{Z}.$$

Следующее утверждение показывает, что как R -модули алгебра Хопфа $R[x]^\circ$ и биалгебра $R[x]^{\circ\circ}$, дуальные к алгебре Хопфа и биалгебре многочленов от k переменных (см. пример 1), совпадают с R -модулем $\mathcal{L}R^{(k)}$ всех k -ЛРП над кольцом R .

Предложение 5. Пусть A — алгебра многочленов $R[x]$ или $R[x, x^{-1}]$ над коммутативным кольцом R с единицей, K — R -подмодуль в A . Тогда условия (a)–(d) предложения 1 эквивалентны. Справедливы равенства

$$R[x]^* \equiv R^{(k)}, \quad R[x]^\circ \equiv \mathcal{L}R^{(k)}, \quad R[x, x^{-1}]^* \equiv R_{bi}^{(k)}, \quad R[x, x^{-1}]^\circ \equiv \mathcal{L}R_{bi}^{(k)} \equiv \mathcal{L}R_{rev}^{(k)}.$$

Доказательство. Импликации (a) $\Rightarrow$ (b) $\Rightarrow$ (c) очевидны. Пусть $A = R[x]$. Тогда импликация (d) $\Rightarrow$ (a) также очевидна. Докажем импликацию (b) $\Rightarrow$ (d) (доказательство отличается от доказательства утверждения 1 и аналогично доказательству утверждения 1.13 из [17]). Пусть R -модуль $R[x]/I$ порождается элементами $\bar{F}_1, \dots, \bar{F}_n$, где $\bar{F} = F + I$. Тогда

$$\bar{x}_1 \bar{F}_j(x) = \sum_i c_{ij} \bar{F}_i$$

для некоторых $c_{ij} \in R$, $1 \leq i, j \leq n$. Рассмотрим матрицу $C = (c_{ij}) \in R_n$. Если $c = (c_1, \dots, c_n)$ — вектор коэффициентов в разложении элемента $\bar{G} \in R[x]/I$ в системе образующих $\bar{F}_1, \dots, \bar{F}_n$, то cC — вектор коэффициентов в разложении элемента $\bar{x}_1 \bar{G}$. Пусть c — вектор коэффициентов в разложении элемента $\bar{1}$. Тогда последовательность векторов $c, cC, cC^2, \dots$, являющихся векторами коэффициентов в разложении элементов $\bar{1}, \bar{x}_1, \bar{x}_1^2, \dots$, аннулируется характеристическим многочленом $\chi_C(x)$ матрицы C . Следовательно, $\bar{\chi}_C(x_1) = 0$, то есть $\chi_C(x_1) \in I$. Таким образом, I содержит унитарный многочлен от переменной x_1 . Аналогично доказывается, что I содержит унитарный многочлен от x_s , $1 \leq s \leq k$, то есть I унитарен.

Пусть теперь $A = R[x, x^{-1}]$. Докажем, что (b) $\Rightarrow$ (d). Пусть R -модуль $R[x, x^{-1}]/I$ порождается элементами $\bar{F}_1, \dots, \bar{F}_n$, где $\bar{F} = F + I$. Рассуждая как и выше, построим матрицу C и унитарный многочлен $\chi_C(x_1) \in I$. Достаточно доказать, что многочлен $\chi_C(x)$ реверсивен, то есть что матрица C обратима. Пусть

$$\bar{x}_1^{-1} \bar{F}_j(x) = \sum_i b_{ij} \bar{F}_i, \quad b_{ij} \in R, \quad 1 \leq i, j \leq n,$$

и пусть $B = (b_{ij})$. Равенства

$$x_1^{-1} x_1 F_j(x) = F_j(x), \quad 1 \leq j \leq n,$$

показывают, что $CB = E$. Поэтому матрица C обратима.

Докажем, что (d) $\Rightarrow$ (a). Пусть выполняется условие (d) и $m_s = \deg F_s(x)$. Докажем, что $R[x, x^{-1}]/I$ — конечно порожденный свободный R -модуль с базисом $x^i + I$, $i \in \Pi = \Pi(m)$. Действительно, очевидно, что $x^i + I$, $i \in \Pi$ — система образующих. Если эти элементы линейно зависимы над R , то идеал I содержит ненулевой многочлен вида

$$H(x) = \sum_{i \in \Pi} c_i x^i.$$

Тогда $H(x)$ должен аннулировать импульсную k -бипоследовательность семейства $L_R^{bi}(F)$, что невозможно.

Отметим, что если дуальные алгебры рассматривать относительно модуля M , то есть положить $A^* = \text{Hom}_R(A, M)$ и A° определить так же, как в (7), то из предложения 5 вытекают равенства

$$\begin{aligned} R[x]^* &\equiv M^{(k)}, & R[x]^\circ &\equiv \mathcal{L}M^{(k)}, \\ R[x, x^{-1}]^* &\equiv M_{\text{bi}}^{(k)}, & R[x, x^{-1}]^\circ &\equiv \mathcal{L}M_{\text{bi}}^{(k)} \equiv \mathcal{L}M_{\text{rev}}^{(k)}. \end{aligned}$$

Так же, как в случае $k = 1$, определим биалгебру $R[x]^{\circ\circ}$ и алгебры Хопфа $R[x]^\circ$ и $R[x, x^{-1}]^{\circ\circ}$ k -линейных рекуррентных (би)последовательностей:

$$\begin{aligned} (R[x]^\circ, *, e_*, \Delta, \varepsilon, S) &\equiv \mathcal{L}R^{(k)}, \\ (R[x]^{\circ\circ}, \cdot, e^\bullet, \Delta, \varepsilon) &\equiv \mathcal{L}R^{(k)\bullet}, \\ (R[x, x^{-1}]^{\circ\circ}, \cdot, e^\bullet, \Delta, \varepsilon, S^\bullet) &\equiv \mathcal{L}R_{\text{bi}}^{(k)\bullet} \equiv \mathcal{L}R_{\text{rev}}^{(k)\bullet}. \end{aligned} \quad (37)$$

В терминах (би)последовательностей операции этих биалгебр задаются следующим образом:

$$(u * v)(i) = \sum_{0 \leq j \leq i} \binom{i}{j} u(j)v(i-j), \quad (uv)(i) = u(i)v(i), \quad (38)$$

$$e_*(i) = \delta_{0i}, \quad e^\bullet(i) = 1, \quad \varepsilon(u) = u(0), \quad S(u)(i) = (-1)^i u(i), \quad S^\bullet(u)(i) = u(-i),$$

где $\binom{i}{j} = \binom{i_1}{j_1} \dots \binom{i_k}{j_k}$, δ_{0i} — символ Кронекера, $(-1)^i = (-1)^{i_1 + \dots + i_k}$ и отношение частичного порядка $\leq$ на множестве $\mathbb{Z}^k$ задается следующим образом:

$$j \leq i \iff j_1 \leq i_1, \dots, j_k \leq i_k.$$

Коумножение Δu определяется условием

$$\Delta u = \sum_u u_{(1)} \otimes u_{(2)} \iff \forall i, j \quad \sum_u u_{(1)}(i)u_{(2)}(j) = u(i+j),$$

или в сокращенной записи

$$\Delta u(i \otimes j) = u(i+j). \quad (39)$$

Если $u \in L_R(F)$ или $u \in L_R^{\text{bi}}(F)$, то верно равенство (см. предложение 2)

$$\Delta u = \sum_{t \in \Pi(m)} e_t^F \otimes x^t u.$$

Ввиду (39) Δu можно рассматривать как $2k$ -(би)последовательность со знаками

$$\Delta u(i, j) = u(i+j).$$

При такой интерпретации $\Delta u \in L_R(F, F)$. Естественные отображения

$$\begin{aligned} R[x]^\circ \otimes \dots \otimes R[x]^\circ &\rightarrow R[x]^\circ, \\ R[x, x^{-1}]^\circ \otimes \dots \otimes R[x, x^{-1}]^\circ &\rightarrow R[x, x^{-1}]^\circ, \end{aligned}$$

при которых элементу $u_1 \otimes \dots \otimes u_k$ сопоставляется k -(би)последовательность u со знаками $u(i) = u_1(i_1) \dots u_k(i_k)$, являются изоморфизмами между k -ми тензорными степенями биагбр (20) и биагбрами (37).

Мы видим, что операции в биагбрах k -линейных рекуррентных (би)последовательностей определяются так же, как в случае $k = 1$, с заменой обозначений на векторные. Легко проверить, что все результаты, полученные выше для 1-последовательностей, переносятся на случай k -последовательностей (за исключением, быть может, предложения 3, требующего дополнительного рассмотрения). Перечислим основные из них.

Групповые элементы биагбр $R[x]^\circ$ и $R[x]^{*\circ}$ — это геометрические прогрессии (a^i) со знаменателями $a \in R^k$, а групповые элементы биагбр $R[x, x^{-1}]^{*\circ}$ и $\mathcal{L}R_{\text{rev}}^{(k)\bullet}$ — это геометрические прогрессии со знаменателями $a \in U(R^k) = U(R)^k$. При этом

$$(a^i) * (b^i) = ((a + b)^i), \quad (a^i)(b^i) = ((ab)^i),$$

и

$$\begin{aligned} (G(R[x]^\circ), *) &\cong (R^k, +), \\ (G(R[x]^{*\circ}), \cdot) &\cong (R^k, \cdot), \\ (G(R[x, x^{-1}]^{*\circ}), \cdot) &\cong (G(\mathcal{L}R_{\text{rev}}^{(k)\bullet}), \cdot) \cong (U(R)^k, \cdot). \end{aligned}$$

Примитивные элементы u в биагбре $R[x]^\circ$ описываются соотношениями $u(0) = u(i) = 0$, если $wt(i) > 1$, где $wt(i) = i_1 + \dots + i_k$ — сумма координат вектора i . Примитивные элементы в биагбрах $R[x]^{*\circ}$, $R[x, x^{-1}]^{*\circ}$ и $\mathcal{L}R_{\text{rev}}^{(k)\bullet}$ — это арифметические прогрессии $u(i) = (a, i) = a_1 i_1 + \dots + a_k i_k$. Во всех случаях группа примитивных элементов относительно сложения изоморфна $(R^k, +)$. Множество интегралов в каждой из биагбр совпадает с множеством (би)последовательностей, кратных (над R) единичному элементу данной биагбры.

Биномиальной k -последовательностью над кольцом R с корнем $a \in R^k$ порядка $n \in \mathbb{N}_0^k$ называется k -последовательность $a^{[n]}$ со знаками

$$a^{[n]}(i) = \binom{i}{n} a^{i-n}. \quad (40)$$

Биномиальная k -последовательность $a^{[n]}$ реверсивна тогда и только тогда, когда $a \in U(R)^k$. В этом случае соотношения (40) определяют продолжение $a^{[n]}$ до биномиальной бипоследовательности $a^{[n]}: \mathbb{Z}^k \rightarrow R$. Легко увидеть, что $a^{[n]}$ есть импульсная (би)последовательность семейства

$$L_R((x - a)^{n+1}) = L_R((x_1 - a_1)^{n_1+1}, \dots, (x_k - a_k)^{n_k+1}).$$

Биномиальная (би)последовательность порядка 0 — это геометрическая прогрессия $a^{[0]}(i) = a^i$. Биномиальные (би)последовательности $a^{[n]}$, $n \in \mathbb{N}_0^k$, удовлетворяют соотношению

$$\Delta a^{[n]} = \sum_{0 \leq j \leq n} a^{[j]} \otimes a^{[n-j]}.$$

Естественные определения конволюции и покоординатного произведения k -ЛРП над кольцом R и k -ЛРП над модулем M задают структуры левого $\mathcal{L}R^{(k)}$ - и $\mathcal{L}R^{(k)\bullet}$ -модулей на

$\mathcal{LM}^{(k)}$. Аналогично покоординатное произведение ЛРБ над R и над M задает структуру левого $\mathcal{LR}_{\text{bi}}^{(k)\bullet}$ -модуля на $\mathcal{LM}_{\text{bi}}^{(k)}$. Определим отображение

$$\rho: \mathcal{LM}^{(k)} \rightarrow \mathcal{LR}^{(k)} \otimes \mathcal{LM}^{(k)}$$

следующим образом: если $u \in L_M(F_1, \dots, F_k)$, $\deg F_s(x) = m_s$, то

$$\rho(u) = \sum_{0 \leq t \leq m-1} e_t^F \otimes x^t u.$$

Для бипоследовательностей ρ определяется аналогично. Тогда модули $\mathcal{LM}^{(k)}$, $\mathcal{LM}_{\text{bi}}^{(k)}$, $\mathcal{LM}_{\text{rev}}^{(k)}$ являются левыми хопфовыми соответственно $\mathcal{LR}^{(k)}$ -, $\mathcal{LR}^{(k)\bullet}$ -, $\mathcal{LR}_{\text{bi}}^{(k)\bullet}$ -, $\mathcal{LR}_{\text{rev}}^{(k)\bullet}$ -модулями относительно структурного отображения ρ .

Произвольной k -последовательности $u \in M^{(k)}$ сопоставим формальный степенной ряд

$$u(x) = \sum_{i \in \mathbb{N}_0^k} u(i) x^i \in M[[x]].$$

Если $u \in L_M(F_1, \dots, F_k)$, $\deg F_s(x) = m_s$, $F_s^{(*)}(x) = x^{m_s} F_s(1/x)$, то $F_s^{(*)}(0) = 1$ и легко видеть, что $F_1^{(*)}(x_1) \dots F_k^{(*)}(x_k) u(x) = H(x)$, где $H(x)$ — многочлен из $M[x]$, степень которого по каждой переменной x_s меньше m_s . С другой стороны, если $G_1(x), \dots, G_k(x) \in R[x]$ — такие многочлены, что $G_s(0) = 1$, то $G_s(x_s)$ обратим как элемент кольца $R[[x]]$ и определен ряд

$$u(x) = 1/(G_1(x_1) \dots G_k(x_k)) = \sum_i u(i) x^i \in R[[x]],$$

коэффициенты которого образуют k -ЛРП $u = (u(i))$ из $L_R(G_1^{(*)}, \dots, G_k^{(*)})$. Отождествляя k -последовательность u с ее производящей функцией $u(x)$, получим, что

$$\mathcal{LM}^{(k)} \equiv M_{\text{rat}}[[x]],$$

где $M_{\text{rat}}[[x]]$ — множество таких рядов $a(x) \in M[[x]]$, что $G_1(x_1) \dots G_k(x_k) a(x)$ принадлежит $M[x]$ для некоторых многочленов $G_1(x), \dots, G_k(x) \in R[x]$, удовлетворяющих условию $G_s(0) = 1$.

Каждая k -ЛРП $u \in L_M(F)$ однозначно представляется в виде $u = \Phi(x) e^F$, где $\Phi(x) \in M[x]$ — многочлен, степень которого по x_s меньше m_s , $s = 1, \dots, k$, называемый генератором k -ЛРП u относительно элементарных характеристических многочленов $F_1, \dots, F_k$. Легко видеть, что

$$F_1^{(*)}(x_1) \dots F_k^{(*)}(x_k) e^F(x) = x^{m-1}.$$

Справедлива формула

$$\Phi^{(*)}(x) = F_1^{(*)}(x_1) \dots F_k^{(*)}(x_k) u(x),$$

где

$$\Phi^{(*)}(x) = x^{m-1} \Phi(x^{-1}) = x_1^{m_1-1} \dots x_k^{m_k-1} \Phi(x_1^{-1}, \dots, x_k^{-1}),$$

или

$$u(x) = \frac{\Phi^{(*)}(x)}{F_1^{(*)}(x_1) \dots F_k^{(*)}(x_k)}.$$

Если кольцо R содержит поле рациональных чисел, то k -последовательности $u \in M^{(k)}$ можно сопоставить экспоненциальную производящую функцию

$$U(x) = \sum_{i \in \mathbb{N}_0^k} u(i) \frac{x^i}{i!} \in M[[x]],$$

где $i! = i_1! \dots i_k!$. Отображение

$$(\mathcal{L}R^{(k)}, *, e_*) \rightarrow (R[[x]], \cdot, 1), \quad u \rightarrow U(x),$$

является мономорфизмом алгебр, то есть конволюции $u * v$ последовательностей отвечает умножение по Коши экспоненциальных производящих функций. Так как

$$x_s(u * v) = (x_s u * v) + (u * x_s v), \quad 1 \leq s \leq k,$$

умножение на x_s (сдвиг k -последовательности влево в s -м направлении) является дифференцированием в алгебре $(\mathcal{L}R^{(k)}, *, e_*)$. При сопоставлении $u \rightarrow U(x)$ умножению k -последовательности на x_s соответствует дифференцирование ряда $U(x)$ по x_s . Следовательно,

$$v = F(x)u \iff V(x) = F\left(\frac{d}{dx}\right)U(x) = F\left(\frac{d}{dx_1}, \dots, \frac{d}{dx_k}\right)U(x).$$

В частности, если $I \subseteq R[x]$, то семейство

$$\mathcal{L}_R(I) = \{u \in \mathcal{L}M^{(k)} : F(x)u = 0 \text{ для всех } F(x) \in I\}$$

можно рассматривать как множество решений системы линейных дифференциальных уравнений

$$F\left(\frac{d}{dx}\right)U(x) = 0, \quad F \in I.$$

Определение линейной и полилинейной рекуррентной последовательности над модулем ${}_R M$ сохраняется в случае, когда кольцо R некоммутативно. Этот случай рассматривался, например, в [18, 19]. Представляет интерес исследование свойств, изложенных в данной статье, в случае некоммутативного основного кольца R . В качестве одного из результатов, приведем следующее утверждение, устанавливающее связь между линейными рекуррентами и представляющими функциями.

Предложение 6. Пусть R — кольцо с единицей. Тогда любая k -ЛРП над модулем ${}_R M$ является представляющей функцией на полугруппе $G = (\mathbb{N}_0^k, +)$ со значениями в M . Если кольцо R нетерово слева, или коммутативно, или если $k = 1$, то верно обратное утверждение.

Доказательство. Если u — k -ЛРП с элементарными характеристическими многочленами $F_1(x_1), \dots, F_k(x_k)$ степеней $m_1, \dots, m_k$ соответственно, то модуль сдвигов $R[x]u$ порождается как R -модуль конечным числом элементов $x^i u$, $0 \leq i \leq m - 1$. Следовательно, u — представляющая функция.

Пусть теперь $u \in M^{(k)}$ — k -последовательность, являющаяся представляющей функцией, то есть R -модуль $R[x]u$ конечно порожден.

Если R нетерово слева, то для любого $s \in \{1, \dots, k\}$ подмодуль ${}_R(u, x_s u, x_s^2 u, \dots)$ модуля сдвигов конечно порожден. Следовательно, $x_s^{m_s} u$ линейно выражается над R через

$u, x_s u, \dots, x_s^{m_s-1} u$ для некоторого $m_s \geq 1$. Это означает, что $\text{An}(u)$ содержит унитарный многочлен $F_s(x_s)$ степени m_s , $1 \leq s \leq k$, то есть u — k -ЛРП.

Пусть R коммутативно. По условию R -модуль $R[x]u$ порождается конечным числом элементов $F_1(x)u, \dots, F_n(x)u$. Тогда

$$x_1 F_j(x)u = \sum_i a_{ij} F_i(x)u$$

для некоторых $a_{ij} \in R$, $1 \leq i, j \leq n$. Рассмотрим матрицу $A = (a_{ij}) \in R_n$. Если $c = (c_1, \dots, c_n)$ — вектор коэффициентов в разложении элемента $G(x)u \in R[x]u$ в системе образующих $F_1(x)u, \dots, F_n(x)u$, то cA — вектор коэффициентов в разложении элемента $x_1 G(x)u$. Пусть c — вектор коэффициентов в разложении элемента u . Тогда последовательность векторов $c, cA, cA^2, \dots$, являющихся векторами коэффициентов в разложении элементов $u, x_1 u, x_1^2 u, \dots$, аннулируется характеристическим многочленом $\chi_A(x)$ матрицы A . Отсюда следует, что $\chi_A(x_1)u = 0$. Таким образом, $\text{An}(u)$ содержит унитарный многочлен от переменной x_1 . Аналогично доказывается, что $\text{An}(u)$ содержит унитарный многочлен от x_s , $1 \leq s \leq k$, то есть u есть k -ЛРП.

В случае $k = 1$

$$R[x]u = R(u, xu, \dots, x^{m-1}u)$$

для некоторого $m \geq 1$. Это условие равносильно тому, что u — ЛРП порядка m .

Справедливо также утверждение о том, что k -линейная рекуррентная бипоследовательность над модулем ${}_R M$ является представляющей функцией на полугруппе $G = \mathbf{Z}^k$ со значениями в M . Если кольцо R нетерово слева, или коммутативно, или если $k = 1$, то верно обратное утверждение. Таким образом, при выполнении последнего условия верны равенства

$$\mathcal{R}(M^{\mathbf{N}_0^k}) = \mathcal{L}M^{(k)}, \quad \mathcal{R}(M^{\mathbf{Z}^k}) = \mathcal{L}M_{\text{bi}}^{(k)}.$$

Список литературы

1. Артамонов В. А., Строение алгебр Хопфа. *Итоги науки и техники. Алгебра, геометрия, топология* (1991) **29**, 3–63.
2. Бахтурин Ю. А., *Основные структуры современной алгебры*. Наука, Москва, 1990.
3. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, ч. II. Гелиос, Москва, 2003.
4. Куракин В. Л., Конволюция линейных рекуррентных последовательностей. *Успехи матем. наук* (1993) **48**, №4, 235–236.
5. Куракин В. Л., Строение алгебр Хопфа линейных рекуррентных последовательностей. *Успехи матем. наук* (1993) **48**, №5, 177–178.
6. Куракин В. Л., Алгебры Хопфа линейных рекуррентных последовательностей над коммутативными кольцами. *Труды Вторых математических чтений МГСУ*. Москва, 1994, с. 67–69.
7. Куракин В. Л., Алгебра Хопфа, дуальная к алгебре многочленов над коммутативным кольцом. *Матем. заметки* (2002) **71**, №5, 677–685.
8. Лидл Р., Нидеррайтер Г., *Конечные поля*, т. 2. Мир, Москва, 1988.
9. Цирлер Н., Линейные возвратные последовательности. *Киберн. сб.* (1963) **6**, 55–79.
10. Abe E., *Hopf algebras*. Cambridge Univ. Press, Cambridge, 1980.
11. Abuhlail J. Y., Gómez-Torrecillas J., Wisbauer R., Dual coalgebras of algebras over commutative rings. *J. Pure and Appl. Algebra* (2000) **153**, 107–120.

12. Abuhlail J. Y., Gómez-Torrecillas J., Lobillo F., Duality and rational modules in Hopf algebras over commutative rings. *J. Algebra* (2001) **240**, 165–184.
13. Cerlienco L., Piras F., On the continuous dual of a polynomial bialgebra. *Commun. Algebra* (1991) **19**, №10, 2707–2727.
14. Cerruti U., Vaccarino F., R -algebras of linear recurrent sequences. *J. Algebra* (1995) **175**, 332–338.
15. Chin W., Goldman J., Bialgebras of lineary recursive sequences. *Commun. Algebra* (1993) **21**, №11, 3935–3952.
16. Haukkanen P., On a convolution of linear recurring sequences over finite fields. I, II. *J. Algebra* (1992) **149**, №1, 179–182; (1994) **164**, №2, 542–544.
17. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
18. Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyshev V. N., Linear and polylinear recurring sequences over abelian groups and modules. *J. Math. Sci.* (2000) **102**, №6, 4598–4627.
19. Kurakin V. L., Nechaev A. A., Quasi-Frobenius bimodules of functions on a semigroup. *Commun. Algebra* (2001) **29**, №9, 4079–4094.
20. Larson R., Taft E. Y., The algebraic structure of linearly recursive sequences under Hadamard product. *Israel J. Math.* (1990) **72**, 118–132.
21. Montgomery S. *Hopf algebras and their actions on rings*. AMS, Providence, 1993.
22. Peterson B., Taft E. Y., The Hopf algebra of linear recursive sequences. *Aequat. Math.* (1980) **20**, 1–17.
23. Snapper E., Completely primary rings, I. *Ann. Math.* (1950) **52**, №3, 666–693.
24. Sweedler M. F., *Hopf algebras*. Benjamin, New York, 1969.
25. Taft E., Algebraic aspects of linearly recursive sequences. *Lect. Notes Pure Appl. Math.* (1994) **158**, 299–317.
26. Taft E., Linearly recursive tableaux. *Congr. Numerantium* (1995) **107**, 33–36.
27. Zierler N., Mills W. H., Products of linear recurring sequences. *J. Algebra* (1973) **27**, №1, 147–157.

Статья поступила 18.04.2003.