Алгебры Хопфа линейных рекуррентных последовательностей над кольцами и модулями

В. Л. КУРАКИН

УДК 512.667.7+511.216

Ключевые слова: алгебра Хопфа, линейная рекуррентная последовательность, линейная рекуррентная бипоследовательность.

Аннотация

Модуль линейных рекуррентных последовательностей над коммутативным кольцом R можно рассматривать как алгебру Хопфа, дуальную к алгебре многочленов над кольцом R. При этом ряд понятий и операций из теории алгебр Хопфа получают интересную интерпретацию в терминах линейных рекуррентных последовательностей. Рассматриваются также некоторые обобщения: линейные рекуррентные бипоследовательности, последовательности над модулем и k-последовательности.

Abstract

V. L. Kurakin, Hopf algebras of linear recurring sequences over rings and modules, Fundamentalnaya i prikladnaya matematika, vol. 9 (2003), no. 1, pp. 113—148.

The module of linear recurring sequences over a commutative ring R can be considered as a Hopf algebra dual to the polynomial Hopf algebra over R. Under this approach, some notions and operations from the Hopf algebra theory have an interesting interpretation in terms of linear recurring sequences. Generalizations are also considered: linear recurring bisequences, sequences over modules, and k-sequences.

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

$$u(i+m) = c_{m-1}u(i+m-1) + \ldots + c_1 u(i+1) + c_0 u(i), \quad i \geqslant 0. \tag{1}$$

Многочлен $F(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1 x - c_0 \in R[x]$ называется *характеристическим многочленом* ЛРП u, а вектор $u(\overline{0, m-1}) = (u(0), \ldots, u(m-1)) \in \in M^m$ — её *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 $\mathcal{L}M^{\langle 1\rangle}$, а множество всех последовательностей над M — через $M^{\langle 1\rangle}$. Многочлен $F(x)$ называется *реверсивным*, если его свободный член $F(0)$ является обратимым элементом кольца R. ЛРП называется *реверсивной*, если у неё существует реверсивный характеристический многочлен. Множество всех реверсивных ЛРП над M обозначим $\mathcal{L}M^{\langle 1\rangle}_{\mathrm{rev}}$.

Фундаментальная и прикладная математика, 2003, том 9, № 1, с. 113—148.

В работе [13] показано, что множество $\mathcal{L}P^{\langle 1\rangle}$ ЛРП над полем P образует алгебру Хопфа, дуальную к алгебре $P[x]$ многочленов над P. Операция умножения в этой алгебре есть конволюция последовательностей. В [9] показано, что на множестве $\mathcal{L}P^{\langle 1\rangle}$ структуру биалгебры можно ввести двумя различными способами, при которых умножение последовательностей задаётся как их конволюция или покоординатное произведение. Операция конволюции ЛРП изучалась независимо в [3] и [9], покоординатное произведение ЛРП исследовалось значительно ранее в [16]. Ещё одна операция конволюции ЛРП, не рассматриваемая в этой работе, изучалась в [10]. Строение алгебры Хопфа $\mathcal{L}P^{\langle 1\rangle}$ исследовано в [4]. В [8] показано, что алгебра Хопфа, дуальная к алгебре $P[x_1,\dots,x_k]$ многочленов от k переменных над полем P, является алгеброй $\mathcal{L}P^{\langle k\rangle}$ всех k-линейных рекуррентных последовательностей (см. ниже раздел 7).

Для исследования алгебры линейных рекуррентных последовательностей над коммутативным кольцом R как алгебры Хопфа, дуальной к алгебре многочленов $R[x]$, требуется предварительно обосновать корректность определения операций в дуальной алгебре $R[x]^\circ$. Как известно [1], для произвольной алгебры Хопфа A над коммутативным нётеровым кольцом дуальная алгебра Хопфа A° определена корректно. В случае алгебры многочленов $A = R[x]$ над коммутативным нётеровым кольцом R это доказано также в [7]. Ранее в [5] без доказательства был сформулирован результат о том, что алгебра Хопфа, дуальная к алгебре многочленов над произвольным коммутативным кольцом R, есть корректно определённая алгебра Хопфа $\mathcal{L}R^{\langle 1\rangle}$ всех ЛРП над R, в явном виде выписаны операции этой алгебры и выделена подалгебра реверсивных последовательностей. Целью данной статьи является более подробное изложение и развитие результатов работы [5], связанных с рассмотрением этой алгебры как алгебры линейных рекуррентных последовательностей. Корректность операций в алгебрах Хопфа, дуальных к алгебрам многочленов $R[\boldsymbol{x}]$ и $R[\boldsymbol{x},\boldsymbol{x}^{-1}]$ над коммутативным кольцом R, доказывается в отдельной статье [6].

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 алгебра Хопфа $R[x]^\circ$ и биалгебра $R[x]^{\bullet\circ}$ оказываются алгеброй Хопфа $\mathcal{L}R^{\langle 1\rangle}$ и биалгеброй $\mathcal{L}R^{\langle 1\rangle\bullet}$ линейных рекуррентных последовательностей, в которых умножение задаётся 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 $R[x,x^{-1}]^{\bullet\circ}$ есть алгебра $\mathcal{L}R_{\mathrm{bi}}^{\langle 1\rangle\bullet}$ линейных рекуррентных бипоследовательностей над кольцом R, которая оказывается изоморфной подалгебре Хопфа $\mathcal{L}R_{\mathrm{rev}}^{\langle 1\rangle\bullet}$ реверсивных последовательностей в биалгебре $\mathcal{L}R^{\langle 1\rangle\bullet}$.

Основные понятия, связанные с алгебрами Хопфа, можно найти в работах [1, 2, 13, 15]. Линейные рекуррентные последовательности над кольцами и модулями рассматриваются в [11,12]. Ниже мы приводим 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.

1. Алгебры Хопфа и дуальные алгебры

Всюду ниже R — основное коммутативное кольцо с единицей 1. Термин «отображение» в дальнейшем означает R-линейной отображение, т. е. гомоморфизм R-модулей, Hom и $\otimes$ означают Hom_R и $\underset{R}{\otimes}$ соответственно. Через 1_A обозначается тождественное отображение $A \to A$. 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:

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

Другими словами, коммутативны диаграммы

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "1_A \otimes m"] \arrow[d, "m \otimes 1_A"'] & A \otimes A \arrow[d, "m"] \\ A \otimes A \arrow[r, "m"] & A \end{tikzcd} \qquad \begin{tikzcd} R \otimes A \arrow[r, leftrightarrow] \arrow[d, "e \otimes 1_A"'] & A \arrow[r, leftrightarrow] \arrow[d, "1_A"'] & A \otimes R \arrow[d, "1_A \otimes e"] \\ A \otimes A \arrow[r, "m"] & A & A \otimes A \arrow[l, "m"'] \end{tikzcd}$$

где $\leftrightarrow$ 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 $t\colon A \otimes A \to A \otimes A$, $a \otimes b \to b \otimes a$, — 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:

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

Другими словами, коммутативны диаграммы

$$
\begin{tikzcd}
C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C \otimes C \arrow[d, "\Delta\otimes 1_C"] \\
C \otimes C \arrow[r, "1_C\otimes\Delta"] & C \otimes C \otimes C
\end{tikzcd}
\qquad
\begin{tikzcd}
C \otimes C \arrow[d, "\varepsilon\otimes 1_C"'] & C \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, "1_C"'] & C \otimes C \arrow[d, "1_C\otimes\varepsilon"] \\
R \otimes C \arrow[r, leftrightarrow] & C \arrow[r, leftrightarrow] & C \otimes R
\end{tikzcd}
$$

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

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

В этих обозначениях законы коассоциативности и коунитарности таковы:

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

Коалгебра C называется *кокоммутативной*, если $t\Delta = \Delta$, где $t\colon C\otimes C \to C\otimes C$ — 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) $\Delta\colon A \to A \otimes A$ — гомоморфизм R-алгебр и

(2) $\varepsilon\colon A \to R$ — гомоморфизм R-алгебр.

Таким образом, $\Delta(ab) = \Delta(a)\Delta(b)$, $\Delta(1) = 1 \otimes 1$ и $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$, $\varepsilon(1) = 1$, где $a, b \in A$. Биалгебра обозначается $(A, m, e, \Delta, \varepsilon)$.

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

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

Таким образом, коммутативна диаграмма

$$
\begin{tikzcd}
A \otimes A \arrow[dd, "S\otimes 1_A"'] & A \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, "\varepsilon"'] & A \otimes A \arrow[dd, "1_A\otimes S"] \\
& R \arrow[d, "e"'] & \\
A \otimes A \arrow[r, "m"] & A & A \otimes A \arrow[l, "m"']
\end{tikzcd}
$$

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 *коподалгеброй*, если $\Delta(L) \subseteq L \otimes L$. Подалгебра L биалгебры A, являющееся коподалгеброй, называется *биподалгеброй*. 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 $R[x]^\bullet = (R[x], \cdot, 1, \Delta_x^\bullet, \varepsilon_x^\bullet)$, полагая

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

Чтобы ввести на биалгебре $R[x]^\bullet$ структуру алгебры Хопфа, рассмотрим её как подалгебру в алгебре $R[x, x^{-1}]$ многочленов Лорана вида $F(x) = \sum\limits_{s=-m}^{n} a_i x^i$, $a_i \in R$, где $m, n \in \mathbb{N}_0$. Введём структуру алгебры Хопфа $R[x, x^{-1}]^\bullet = (R[x, x^{-1}], \cdot, 1, \Delta_x^\bullet, \varepsilon_x^\bullet, S_x^\bullet)$, полагая

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

Таким образом, $\Delta_x^\bullet(x^i) = x^i \otimes x^i$ и $S_x^\bullet(x^i) = x^{-i}$, $i \in \mathbb{Z}$. При этом $R[x]^\bullet$ — биподалгебра в алгебре Хопфа $R[x, x^{-1}]^\bullet$. Проверка того, что введённые 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, причём $a^{-1} = S(a)$, $a \in G(A)$. 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 приведённом выше примере две структуры биалгебры на $R[x]$ задаются так, что x оказывается примитивным или групповым элементом соответственно.

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

$$\begin{gathered}
\Delta_x(F) = F(\boldsymbol{x} \otimes \mathbf{1} + \mathbf{1} \otimes \boldsymbol{x}) = F(x_1 \otimes 1 + 1 \otimes x_1, \ldots, x_k \otimes 1 + 1 \otimes x_k),\\
\Delta_x^\bullet(F) = F(\boldsymbol{x} \otimes \boldsymbol{x}) = F(x_1 \otimes x_1, \ldots, x_k \otimes x_k),\\
\varepsilon_x(F) = F(\mathbf{0}), \quad \varepsilon_x^\bullet(F) = F(\mathbf{1}), \quad S_x(F) = F(-\boldsymbol{x}),
\end{gathered} \tag{3}$$

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

Пусть $R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ — алгебра многочленов вида $F(\boldsymbol{x}) = \sum\limits_{\boldsymbol{s} \in \mathbb{Z}^k} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}}$, где лишь конечное число коэффициентов $c_{\boldsymbol{s}} \in R$ отличны от 0. На этой алгебре можно ввести структуру алгебры Хопфа $(R[\boldsymbol{x}, \boldsymbol{x}^{-1}], \cdot, 1, \Delta_x^\bullet, \varepsilon_x^\bullet, S_x^\bullet)$, в которой $\Delta_x^\bullet$ и $\varepsilon_x^\bullet$ определяются так же, как в (3), и

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

Отметим, что естественные отображения

$$R[x] \otimes \ldots \otimes R[x] \to R[\boldsymbol{x}], \quad R[x, x^{-1}] \otimes \ldots \otimes R[x, x^{-1}] \to R[\boldsymbol{x}, \boldsymbol{x}^{-1}],$$

задаваемые правилом $F_1(x) \otimes \ldots \otimes F_k(x) \to F_1(x_1) \ldots F_k(x_k)$, 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* $C^* = \mathrm{Hom}(C, R)$ зададим структуру алгебры. Операция умножения на C^*, обозначаемая $*$ или m, определяется следующим образом: если $u, v \in C^*$, то

$$u * v = m_R(u \otimes v)\Delta, \tag{4}$$

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

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

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

$$e \colon R \to C^*, \quad e(1) = \varepsilon. \tag{6}$$

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 $\Delta \colon C \to C \otimes C$ и коединице $\varepsilon \colon C \to R$:

$$\Delta^* \colon (C \otimes C)^* \to C^*, \quad \varepsilon^* \colon R^* \to C^*.$$

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

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

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

$$\alpha \colon C^* \otimes C^* \to (C \otimes C)^*, \quad \beta \colon R \to R^* \text{ —}$$

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 $r,r'\in R$, причём $\alpha(u\otimes v)$ — 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

$$m(u\otimes v)=\Delta^*(\alpha(u\otimes v))=\Delta^*(m_R(u\otimes v))=m_R(u\otimes v)\Delta,$$
$$e(1)=\varepsilon^*(\beta(1))=\varepsilon^*(\hat 1)=\hat 1\varepsilon=\varepsilon,$$

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

Рассмотрим двойственную ситуацию. Пусть (A,m,e) — алгебра, и пусть $A^*=\mathrm{Hom}(A,R)$. Ядро $\mathrm{Ker}\,u$ 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 порождённый проективный R-модуль. Таким образом,

$$A^\circ=\{u\in A^*\colon\ \mathrm{Ker}\,u\supseteq I,\ I\lhd A,\ A/I\in\mathbf{P}(R)\},\tag{7}$$

где $\mathbf{P}(R)$ — множество конечно порождённых проективных R-модулей. Предположим, что ограничение определённого выше отображения $\alpha\colon A^*\otimes A^*\to(A\otimes A)^*$ 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:

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

Эти условия задают элемент 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

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

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

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

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 $m\colon A\otimes A\to A$ и единице $e\colon R\to A$, имеют вид

$$m^*\colon A^*\to (A\otimes A)^*,\qquad m^*(\varphi)=\varphi m,$$
$$e^*\colon A^*\to R^*,\qquad e^*(\varphi)=\varphi e,\quad \varphi\in A^*.$$

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

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

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 $\alpha\colon A^\circ\otimes A^\circ\to (A\otimes A)^\circ$ — изоморфизм, выполнено по крайней мере в двух случаях: если кольцо R нётерово (см. [1]) или если A — алгебра многочленов $R[\boldsymbol{x}]$ или $R[\boldsymbol{x},\boldsymbol{x}^{-1}]$ над коммутативным кольцом R (см. [6]; в случае кольца многочленов $R[x]$ над нётеровым кольцом см. [7]). Отметим, что в [1] при определении коалгебры, дуальной к алгебре, пропущено условие нётеровости кольца R.

Пусть $(A,m_A,e_A,\Delta_A,\varepsilon_A)$ — биалгебра. Предположим, что кольцо R нётерово или что A — биалгебра многочленов $R[\boldsymbol{x}]$ или $R[\boldsymbol{x},\boldsymbol{x}^{-1}]$ 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 $m(A^\circ\otimes A^\circ)\subseteq A^\circ$, т. е. A° — подалгебра в A^*, и $(A^\circ,m,e,\Delta,\varepsilon)$ — биалгебра, называемая *дуальной к биалгебре* A. Если дополнительно A — алгебра Хопфа с антиподом $S_A\colon A\to A$, то A° оказывается алгеброй Хопфа с антиподом

$$S\colon A^\circ\to A^\circ,\quad S^\circ(u)=uS_A, \tag{11}$$

являющимся ограничением отображения $S_A^*\colon A^*\to A^*$, 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, 6, 7].

2. Последовательности и бипоследовательности

Для последовательности $u\in M^{\langle 1\rangle}$ обозначим через $x^s u=(u(s),u(s+1),\ldots)$ сдвиг u на s шагов влево. Определим умножение многочлена $F(x)=\sum\limits_{s\geqslant 0} c_s x^s\in$

$\in R[x]$ на последовательность $u \in M^{\langle 1 \rangle}$ как последовательность $F(x)u \in M^{\langle 1 \rangle}$ вида

$$F(x)u = \sum_s c_s x^s u, \quad \text{т. е. } (F(x)u)(i) = \sum_s c_s u(i+s), \quad i \geqslant 0. \tag{12}$$

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

$$\mathrm{An}(u) = \{F(x) \in R[x]\colon\ F(x)u = 0\} \lhd R[x]$$

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

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

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

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

$$R[x]^* \equiv R^{\langle 1 \rangle}. \tag{13}$$

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

$$F(x)\hat{u} = \hat{u}\hat{F}, \quad \text{т. е. } (F(x)\hat{u})(G) = \hat{u}(FG), \quad G \in R[x], \tag{14}$$

где $\hat{F}\colon R[x] \to R[x]$ — 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 $i \geqslant 0$, т. е.

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

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

Бипоследовательностью над модулем M назовём произвольную функцию $u\colon \mathbb{Z} \to M$. Множество всех бипоследовательностей над M обозначим $M_{\mathrm{bi}}^{\langle 1 \rangle}$. Бипоследовательность u будем называть *линейной рекуррентной бипоследовательностью* (ЛРБ) порядка m над модулем M, если существуют элементы $c_0, \ldots, c_{m-1} \in R$, такие что c_0 — обратимый элемент кольца R и условие (1) выполняется для всех $i \in \mathbb{Z}$. Многочлен $F(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1 x - c_0 \in R[x]$

будем называть *характеристическим многочленом* ЛРБ u. Этот многочлен реверсивен. Вектор $u(\overline{0,m-1}) = (u(0),\ldots,u(m-1)) \in R^m$ назовём *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 $L_M^{\mathrm{bi}}(F)$, а множество всех ЛРБ над M — через $\mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle}$.

Бипоследовательность $u^*\colon \mathbb{Z} \to M$, определяемую равенствами $u^*(i) = u(-i)$, $i \in \mathbb{Z}$, назовём *реверсом* бипоследовательности u. Если $u \in L_M^{\mathrm{bi}}(F)$, то $u^* \in L_M^{\mathrm{bi}}(F^*)$, где $F^*(x) = x^m F(0)^{-1} F(1/x)$ — многочлен, сопряжённый 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 $u \in L_M^{\mathrm{bi}}(F)$, т. е. так, чтобы соотношение (1) выполнялось для всех $i \in \mathbb{Z}$. *Реверсом* реверсивной ЛРП u назовём ЛРП $u^*\colon \mathbb{N}_0 \to M$ со знаками $u^*(i) = u(-i)$, $i \geqslant 0$. 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 $v(\overline{0,m-1}) = (u(m-1),\ldots,u(0))$; тогда $u^* = x^{m-1}v$.

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

$$\mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle} \equiv \mathcal{L}M_{\mathrm{rev}}^{\langle 1\rangle}. \tag{16}$$

Пусть $x^s u$ — сдвиг бипоследовательности u на s шагов влево: $(x^s u)(i) = u(i+s)$, $i \in \mathbb{Z}$. На абелевой группе $(M_{\mathrm{bi}}^{\langle 1\rangle}, +)$ зададим структуру левого $R[x,x^{-1}]$-модуля, определив умножение многочлена $F(x) = \sum\limits_{s=-m}^{n} c_s x^s \in R[x,x^{-1}]$ на бипоследовательность u правилом (12). Отметим, что ввиду (16) это определение индуцирует структуру $R[x,x^{-1}]$-модуля также на множестве $\mathcal{L}M_{\mathrm{rev}}^{\langle 1\rangle}$ реверсивных ЛРП, при котором $x^{-s}u$ есть сдвиг ЛРП u на s шагов вправо.

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

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

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

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

$$R[x,x^{-1}]^* \equiv R_{\mathrm{bi}}^{\langle k\rangle}. \tag{17}$$

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

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

Утверждение 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.*

(а) $\exists I \subseteq K,\ I \lhd A,\ A/I$ *— конечно порождённый свободный R-модуль.*

(б) $\exists I \subseteq K,\ I \lhd A,\ A/I$ *— конечно порождённый проективный R-модуль.*

(в) $\exists I \subseteq K,\ I \lhd A,\ A/I$ *— конечно порождённый R-модуль.*

(г) $\exists I \subseteq K,\ I \lhd A,\ I$ *унитарен.*

Доказательство. Импликации (а $\Rightarrow$ б $\Rightarrow$ в) очевидны. Пусть $A = R[x]$. Импликация (в $\Rightarrow$ г) доказана, например, в [14, Statement 10.1]. А именно, пусть R-модуль $R[x]/I$ порождается элементами $F_1 + I, \ldots, F_r + I$, и пусть m — максимальная из степеней многочленов $F_1, \ldots, F_r$. Тогда R-модуль $R[x]/I$ порождается элементами $1{+}I, x{+}I, \ldots, x^m{+}I$. Следовательно, $x^{m+1} - \sum\limits_{i=0}^{m} c_i x^i \in I$ для некоторых $c_i \in R$, т. е. выполнено условие (г). Импликация (г $\Rightarrow$ а) очевидна.

Пусть теперь $A = R[x,x^{-1}]$.

(в $\Rightarrow$ г) Из (в) следует, что R-модуль $R[x,x^{-1}]/I$ порождается конечным числом элементов $x^{-m} + I, x^{-m+1} + I, \ldots, x^m + I$. 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, то многочлен

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

который является унитарным и реверсивным, принадлежит I. При этом $F(x)R[x,x^{-1}] \subseteq I \subseteq K$.

(г $\Rightarrow$ а) 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 порождённый свободный R-модуль с базисом $1{+}I, x{+}I, \ldots, x^{m-1}{+}I$. 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 $\sum\limits_{i=0}^{m-1} r_i x^i \in I$, $r_i \in R$. Обозначим

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

где $g_n \neq 0$, $g_N \neq 0$, $n \leqslant N$. Так как $F(x)$ унитарен, то старший член $H(x)$ есть $g_N x^{m+N} \neq 0$. Так как $F(x)$ реверсивен, то 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 $n \geqslant 0$, что невозможно. $\square$

Следствие 2. *Справедливы равенства*

$$R[x]^* \equiv R^{\langle 1\rangle}, \quad R[x]^\circ \equiv \mathcal{L}R^{\langle 1\rangle},$$
$$R[x,x^{-1}]^* \equiv R^{\langle 1\rangle}_{\mathrm{bi}}, \quad R[x,x^{-1}]^\circ \equiv \mathcal{L}R^{\langle 1\rangle}_{\mathrm{bi}} \equiv \mathcal{L}R^{\langle 1\rangle}_{\mathrm{rev}}.$$

3. Алгебры Хопфа линейных рекуррентных последовательностей

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

$$\begin{aligned}&(R[x],\cdot,1,\Delta_x,\varepsilon_x,S_x),\\&(R[x]^\bullet,\cdot,1,\Delta^\bullet_x,\varepsilon^\bullet_x),\\&(R[x,x^{-1}]^\bullet,\cdot,1,\Delta^\bullet_x,\varepsilon^\bullet_x,S^\bullet_x).\end{aligned} \tag{18}$$

Так как $\Delta_x(x) = x\otimes 1 + 1\otimes x$, $\Delta^\bullet_x(x) = x\otimes x$, то

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

Введём обозначения для операций дуальных биалгебры и алгебр Хопфа:

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

Здесь одинаковые символы обозначают одинаковые операции, возможно, определённые на разных множествах. В частности, поскольку структуры алгебр в биалгебрах (18) одинаковы, то 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 $R[x]^{\bullet\circ}$ — через $m^\bullet$. Эти операции будем называть конволюцией и покоординатным произведением последовательностей соответственно. Операции первых двух биалгебр из (20) имеют следующие области определения и значений (для последней алгебры Хопфа в (20) соотношения аналогичны):

$$
\begin{aligned}
* = m_*\colon \mathcal{L}R^{\langle 1\rangle} \otimes \mathcal{L}R^{\langle 1\rangle} \to \mathcal{L}R^{\langle 1\rangle} &\quad \text{— конволюция последовательностей,}\\
\cdot = m^\bullet\colon \mathcal{L}R^{\langle 1\rangle} \otimes \mathcal{L}R^{\langle 1\rangle} \to \mathcal{L}R^{\langle 1\rangle} &\quad \text{— покоординатное произведение,}\\
e_*, e^\bullet\colon R \to \mathcal{L}R^{\langle 1\rangle} &\quad \text{— единицы относительно } * \text{ и } \cdot,\\
\Delta\colon \mathcal{L}R^{\langle 1\rangle} \to \mathcal{L}R^{\langle 1\rangle} \otimes \mathcal{L}R^{\langle 1\rangle} &\quad \text{— коумножение,}\\
\varepsilon\colon \mathcal{L}R^{\langle 1\rangle} \to R &\quad \text{— коединица,}\\
S\colon \mathcal{L}R^{\langle 1\rangle} \to \mathcal{L}R^{\langle 1\rangle} &\quad \text{— антипод.}
\end{aligned}
$$

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 $\mathcal{L}R^{\langle 1\rangle}$ или бипоследовательности из $\mathcal{L}R^{\langle 1\rangle}_{\mathrm{bi}}$. Тогда в терминах функций операции дуальных алгебр задаются равенствами

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

В терминах последовательностей эти равенства имеют вид

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

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

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

или в терминах последовательностей

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

Для унитарного многочлена $F(x) \in R[x]$ степени m обозначим через e_t^F, $0 \leqslant t \leqslant m-1$, ЛРП из $L_R(F)$ с начальным вектором $e_t^F(\overline{0, m-1}) = (0, \ldots, 0, 1, 0, \ldots, 0)$, 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 $e_t^F \in L_R^{\mathrm{bi}}(F)$, $0 \leqslant t \leqslant m-1$.

Утверждение 3. *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 $\sum\limits_t e_t^F v(t) = v$. Отсюда

$$\sum_{t=0}^{m-1} e_t^F(i)(x^t u)(j) = \biggl(\sum_{t=0}^{m-1} e_t^F (x^j u)(t)\biggr)(i) = (x^j u)(i) = u(i+j), \qquad (24)$$

что и требовалось доказать. □

Следствие 4. *Если $F(x)$ и $G(x)$ — два характеристических многочлена (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 5. *ЛРП-семейства $L_R(F)$ и $L_R^{\mathrm{bi}}(F)$ являются коподалгебрами в $\mathcal{L}R^{\langle 1\rangle}$ и $\mathcal{L}R_{\mathrm{bi}}^{\langle 1\rangle}$ соответственно.*

Операции коумножения последовательности можно дать следующую интерпретацию. Произвольное отображение $v\colon \mathbb{N}_0^2 \to R$ назовём *2-последовательностью* над кольцом R. 2-последовательность v можно также рассматривать как отображение $\hat{v} \in R[x_1, x_2]^* = \mathrm{Hom}(R[x_1, x_2], R)$. 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. Её 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 6. *Пусть R — коммутативное кольцо с единицей.*

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

(б) *Биалгебра, дуальная к биалгебре многочленов $R[x]^\bullet$, есть биалгебра $R[x]^{\bullet\circ} \equiv \mathcal{L}R^{\langle 1\rangle\bullet}$ всех ЛРП над кольцом R с операцией покоординатного произведения в качестве умножения последовательностей.*

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

Отметим, что множество $\mathcal{L}R_{\mathrm{rev}}^{\langle 1\rangle}$ реверсивных последовательностей не образует подалгебру в алгебре $\mathcal{L}R^{\langle 1\rangle}$, поскольку конволюция двух реверсивных последовательностей $u = (1,-1,1,-1,\ldots)$ и $v = (1,1,1,1,\ldots)$ равна $u * v = (1,0,0,0,\ldots)$ 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 $a,b \in A$:

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

Если A коммутативна, достаточно рассматривать структуру левого A-модуля, при этом

$$a \cdot u = u\hat{a}, \quad \text{где } \hat{a}\colon A \to A \text{ — гомотетия.}$$

В рассматриваемом случае $A = R[x]$ или $A = R[x,x^{-1}]$ с учётом (14) получаем

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

Таким образом, внешнее умножение, определяемое на биалгебрах (20) формулой (25), совпадает со структурами $R[x]$- и $R[x,x^{-1}]$-модулей из раздела 2.

Любая коподалгебра $C \subseteq A^\circ$ является A-подмодулем в A°. Действительно, если $u \in C$, то $\Delta u = \sum_u u_{(1)} \otimes u_{(2)}$, где $u_{(1)}, u_{(2)} \in C$, и ввиду (8) $u(ab) = \sum_u u_{(1)}(a)u_{(2)}(b)$ для любых $a,b \in A$. Последнее равенство можно записать в виде $a \cdot u = \sum_u u_{(1)}(a)u_{(2)}$, откуда следует, что $a \cdot u \in C$, т. е. что C является A-подмодулем в A°. В нашем случае получаем, что *любая коподалгебра $C \subseteq R[x]^\circ$ (или $C \subseteq R[x,x^{-1}]^\circ$) является $R[x]$-подмодулем (или $R[x,x^{-1}]$-подмодулем)*. Сформулированное выше следствие 5 можно рассматривать как частичное обращение этого свойства. Отметим, что если R — поле, то C является коподалгеброй в $R[x]^\circ$ тогда и только тогда, когда C является $R[x]$-подмодулем (см. [4]), но в общем случае это неверно. Например, если $R = \mathbb{Z}_4$,

$u = (2, 2, 2, \ldots) \in L_R(x-1)$, $C = R[x]u = \{0, u\}$, то C является $R[x]$-подмодулем в $R[x]^\circ$, но не коподалгеброй, поскольку $\Delta u = e^{x-1} \otimes u \notin C \otimes C = 0$.

Отображение $m\colon C \otimes A \to A$, $m(c \otimes a) = c \cdot a$, 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 $\Delta c = \sum\limits_c c_{(1)} \otimes c_{(2)}$, выполняются равенства

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

Если при этом C — биалгебра и отображение m задаёт на A структуру левого C-модуля, т. е.

$$(cd) \cdot a = c \cdot (d \cdot a), \quad 1 \cdot a = a \quad (\text{где } d, 1 \in C),$$

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 $m\colon A \otimes A^\circ \to A^\circ$, $m(a \otimes u) = a \cdot u$, определённое 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 2 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

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

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

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

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

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

являющаяся ни 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 $j \in \overline{0, i}$. На самом деле, как показывает следующее утверждение, знаки последовательности $u * v$ можно вычислять рекуррентно, храня в памяти матрицу фиксированного размера $(m \times n)$. В утверждении 7 мы будем считать, что нумерация строк и столбцов матриц начинается с нуля. Элементы матрицы M будем обозначать M_{ij}. Обозначим через $S(F)$ сопровождающую матрицу унитарного многочлена $F(x) = x^m - \sum_{s=0}^{m-1} f_s x^s \in R[x]$:

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

Утверждение 7. *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 $M^{(k)}$ над кольцом R размеров $(m \times n)$, полагая*

$$M_{ij}^{(0)} = u(i)v(j), \quad 0 \leqslant i \leqslant m-1, \quad 0 \leqslant j \leqslant n-1,$$
$$M^{(k+1)} = S(F)^T M^{(k)} + M^{(k)} S(G), \quad k \geqslant 0.$$

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

Доказательство. Докажем индукцией по k, что $M_{ij}^{(k)} = ((x^i u) * (x^j v))(k)$, $0 \leqslant i \leqslant m-1$, $0 \leqslant j \leqslant n-1$. При $k = 0$ имеем

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

Пусть сформулированное утверждение доказано при некотором $k \geqslant 0$. Обозначим $A = S(F)^T M^{(k)}$, $B = M^{(k)} S(G)$. Если $i \in \overline{0, m-2}$, то $A_{ij} = M_{i+1,j}^{(k)} = (x^{i+1} u * x^j v)(k)$. Если же $i = m-1$, то

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

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

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

что доказывает шаг индукции. □

4. 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 $a(x) \in M[[x]]$ назовём *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 $u \in M^{\langle k \rangle}$ сопоставим ряд

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

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

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 увидеть, $G(x)u(x)$ — многочлен степени меньше m, т. е. $u(x)$ — 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 $u \to u(x)$ задаёт взаимно-однозначные соответствия

$$M^{\langle 1 \rangle} \equiv M[[x]], \quad \mathcal{L}M^{\langle 1 \rangle} \equiv M_{\mathrm{rat}}[[x]].$$

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

$$M_{\mathrm{bi}}^{\langle 1 \rangle} \equiv M[[x, x^{-1}]], \quad \mathcal{L}M_{\mathrm{bi}}^{\langle 1 \rangle} \equiv M_{\mathrm{rat}}[[x, x^{-1}]].$$

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

$$(R_{\mathrm{rat}}[[x]], *, e_*, \Delta, \varepsilon, S) \equiv \mathcal{L}R^{\langle 1 \rangle} \equiv R[x]^\circ,$$
$$(R_{\mathrm{rat}}[[x]]^\bullet, \cdot, e^\bullet, \Delta, \varepsilon) \equiv \mathcal{L}R^{\langle 1 \rangle \bullet} \equiv R[x]^{\bullet\circ},$$
$$(R_{\mathrm{rat}}[[x, x^{-1}]]^\bullet, \cdot, e^\bullet, \Delta, \varepsilon, S^\bullet) \equiv \mathcal{L}R_{\mathrm{bi}}^{\langle 1 \rangle \bullet} \equiv \mathcal{L}R_{\mathrm{rev}}^{\langle 1 \rangle \bullet} \equiv R[x, x^{-1}]^{\bullet\circ}.$$

Операции здесь являются операциями (22), (23), (9), выраженными в терминах формальных степенных рядов: если $a(x) = \sum a_i x^i$, $b(x) = \sum b_i x^i$, то

$$\begin{gathered} a(x)*b(x)=\sum_{k\geqslant 0}\sum_{i=0}^{k}\binom{k}{i}a_ib_{k-i}x^k, \quad a(x)\cdot b(x)=\sum_i a_ib_ix^i, \\ \Delta a=\sum_{i,j}a_{i+j}x^i\otimes x^j, \quad e_*=1, \quad e^\bullet=\sum_i x^i, \\ \varepsilon(a)=a(0)=a_0, \quad S(a)=a(-x), \quad S^\bullet(a)=a(x^{-1}). \end{gathered} \tag{29}$$

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

Рациональный ряд $a(x)\in M[[x]]$ назовём *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 $R_{\mathrm{rat}}[[x]]^\bullet_{\mathrm{rev}}$ в биподалгебре $R_{\mathrm{rat}}[[x]]^\bullet$, изоморфную $R_{\mathrm{rat}}[[x,x^{-1}]]^\bullet$.

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 $e^F, xe^F, \ldots, x^{m-1}e^F$ с коэффициентами из M:

$$u=\varphi_0e^F+\varphi_1xe^F+\ldots+\varphi_{m-1}x^{m-1}e^F=\Phi(x)e^F, \quad \text{где } \Phi(x)=\sum_{s=0}^{m-1}\varphi_sx^s\in M[x].$$

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

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

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 $(x^se^F)(x)=x^{-s}e^F(x)$, откуда

$$\begin{aligned} F^{(*)}(x)u(x)&=F^{(*)}(x)\Bigl(\sum_s\varphi_sx^se^F\Bigr)(x)= \\ &=F^{(*)}(x)\sum_s\varphi_sx^{-s}e^F(x)=\sum_s\varphi_sx^{m-1-s}=\Phi^{(*)}(x). \end{aligned}$$

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 мы можем теперь объяснить смысл многочлена $H(x)$. А именно, $H(x) = \Phi^{(*)}(x)$, 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*

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

Экспоненциальный ряд назовём *рациональным*, если соответствующая обыкновенная производящая функция рациональна. Множество рациональных экспоненциальных рядов обозначим $M^{\exp}_{\mathrm{rat}}[[x]]$. Взаимно-однозначное соответствие

$$\mathcal{L}M^{\langle 1\rangle} \equiv M^{\exp}_{\mathrm{rat}}[[x]], \quad u \equiv U(x),$$

при $M = R$ индуцирует структуру алгебры Хопфа

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

со следующими операциями: если $A(x) = \sum a_i \frac{x^i}{i!}$ и $B(x) = \sum b_i \frac{x^i}{i!}$, то

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

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

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

Структура левого $R[x]$-модуля на множестве последовательностей индуцирует структуру левого $R[x]$-модуля на алгебре экспоненциальных производящих функций. Соответствующую внешнюю операцию обозначим $\cdot\colon R[x] \otimes R^{\exp}_{\mathrm{rat}}[[x]] \to R^{\exp}_{\mathrm{rat}}[[x]]$. Если $v = xu$ — сдвиг последовательности u, то соответствующие экспоненциальные производящие функции связаны соотношением

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

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

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

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

$$U^{(n)}(x) = c_{m-1}U^{(n-1)}(x) + \ldots + c_1U'(x) + c_0U(x), \tag{30}$$

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

В алгебрах обыкновенных производящих функций внешнее умножение на x индуцирует эндоморфизм сдвига коэффициентов ряда: $x \cdot a(x) = \sum\limits_{i \geqslant 0} a_{i+1}x^i$ в алгебре $R[x]^\bullet$ и $x \cdot a(x) = \sum\limits_{i \in \mathbb{Z}} a_{i+1}x^i = x^{-1}a(x)$ 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 $u\colon G \to M$. Это множество образует алгебру над кольцом R с поточечными операциями сложения и умножения функций и умножения на скаляры из R. Определим действие группы G на множестве M^G правилом

$$(gu)(h) = u(gh), \quad \text{где } g, h \in G, \quad u \in M^G.$$

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

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

Утверждение 8. (*Би*)*последовательность является представляющей функцией тогда и только тогда, когда она является линейной рекуррентной* (*би*)*последовательностью. Таким образом,*

$$M^{\mathbb{N}_0} = M^{\langle 1 \rangle}, \quad M^{\mathbb{Z}} = M^{\langle 1 \rangle}_{\mathrm{bi}}, \quad \mathcal{R}(M^{\mathbb{N}_0}) = \mathcal{L}M^{\langle 1 \rangle}, \quad \mathcal{R}(M^{\mathbb{Z}}) = \mathcal{L}M^{\langle 1 \rangle}_{\mathrm{bi}}.$$

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

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.

5. Групповые и примитивные элементы, интегралы и разделённые 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 $u(a)u(b) = u(ab)$, $a, b \in A$, т. е. $u\colon A \to R$ — 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

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

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

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

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

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

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

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

$$\begin{gathered}(G(R[x]^\circ), *) \cong (R, +),\\ (G(R[x]^{\bullet\circ}), \cdot) \cong (R, \cdot),\\ (G(R[x, x^{-1}]^{\bullet\circ}), \cdot) \cong (G(\mathcal{L}R^{\langle 1\rangle\bullet}_{\mathrm{rev}}), \cdot) \cong (U(R), \cdot),\end{gathered}$$

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

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

Ввиду (9) последовательность u является примитивным элементом биалгебры $R[x]^\circ$, т. е. $\Delta u = u \otimes e_* + e_* \otimes u$, тогда и только тогда, когда $u(i)e_*(j) + e_*(i)u(j) = u(i+j)$. Так как $e_* = (1,0,0,0,\ldots)$, то отсюда получаем

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

(Би)последовательность u из $R[x]^{\bullet\circ}$, $R[x,x^{-1}]^{\bullet\circ}$ или $\mathcal{L}R^{\langle 1\rangle\bullet}_{\mathrm{rev}}$ 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 $e_* = (1,1,1,1,\ldots)$, то 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 трёх 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 $\hat u \in \mathrm{Hom}(A,R)$, 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 её 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 $u = u(0)e_*$, т. е. u кратна e_*. Обратно, если $u = ae_*$, то $u*v = av = u(0)v = \varepsilon(u)v$, т. е. u — интеграл.

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

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

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

Формулу $a^{[n]}(i) = \binom{i}{n}a^{i-n}$ будем использовать при всех $i \geqslant 0$, 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 $a^{[n]} \in L_R^{\mathrm{bi}}((x-a)^{n+1})$, полагая

$$a^{[n]}(i) = \binom{i}{n} a^{i-n}, \quad i \in \mathbb{Z}, \quad \text{где } \binom{i}{n} = \frac{i(i-1)\ldots(i-n+1)}{n!}, \quad n \geqslant 0.$$

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

Последовательность элементов $c_0, c_1, \ldots$ коалгебры C называется *разделёнными степенями*, если

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

Проверим, что биномиальные (би)последовательности $a^{[n]}$, $n \geqslant 0$, образуют последовательность разделённых степеней в биалгебрах $R[x]^\circ$ и $R[x]^{\bullet\circ}$, а если элемент a обратим, то в биалгебрах $R[x, x^{-1}]^{\bullet\circ}$ и $\mathcal{L}R_{\mathrm{rev}}^{\langle 1\rangle\bullet}$. 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.

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

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

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

$$L_R(F) = L_R((x-a_1)^{m_1}) \dotplus \ldots \dotplus L_R((x-a_t)^{m_t})$$

и является свободным R-модулем с базисом $\{a_s^{[n_s]},\ 0 \leqslant n_s \leqslant m_s - 1,\ 1 \leqslant s \leqslant t\}$, состоящим из биномиальных последовательностей [11]. Если кольцо R содержит поле рациональных чисел, то экспоненциальная производящая функция $A(x)$ биномиальной последовательности $a^{[n]}$ имеет вид

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

Таким образом, биномиальный базис в терминах экспоненциальных производящих функций есть стандартный базис $\frac{x^{n_s}}{n_s!} e^{a_s x}$, $0 \leqslant n_s \leqslant m_s - 1$, $1 \leqslant s \leqslant t$, 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 $\mathrm{Hom}(R[x], R)$ записывается в виде $\hat{a}^{[n]}(x^i) = \binom{i}{n} a^{i-n} = (x^i)^{(n)}(a)/n!$, где верхний индекс (n)

означает n-ю производную. Следовательно, $\hat{a}^{[n]}(F(x)) = F^{(n)}(a)/n!$ — 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

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

причём такая формула Тейлора уже не требует предположения, что R содержит поле рациональных чисел.

6. Хопфов модуль линейных рекуррент над модулем

Выше были рассмотрены структуры биалгебр и алгебр Хопфа на множестве $\mathcal{L}R^{\langle k\rangle}$ ЛРП над кольцом R. В этом разделе мы покажем, что множество $\mathcal{L}M^{\langle 1\rangle}$ всех ЛРП над R-модулем M образуют хопфов модуль над алгеброй $\mathcal{L}R^{\langle 1\rangle}$ всех ЛРП над кольцом R.

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

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

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

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

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 $\rho\colon M \to H \otimes M$, причём для любых $m \in M$ и $h \in H$ при условии $\Delta h = \sum\limits_h h_{(1)} \otimes h_{(2)}$ выполняется соотношение

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

Поскольку множество $\mathcal{L}M^{\langle 1\rangle}$ ЛРП над модулем M является левым $R[x]$-модулем, естественно попытаться задать структурное отображение $\rho\colon \mathcal{L}M^{\langle 1\rangle} \to R[x] \otimes \mathcal{L}M^{\langle 1\rangle}$ так, чтобы превратить $\mathcal{L}M^{\langle 1\rangle}$ 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 $\mathcal{L}M^{\langle 1\rangle}$, $\mathcal{L}M^{\langle 1\rangle}$, $\mathcal{L}M^{\langle 1\rangle}_{\mathrm{bi}}$, $\mathcal{L}M^{\langle 1\rangle}_{\mathrm{rev}}$ являются левыми соответственно $R[x]$-, $R[x]^{\bullet}$-,

$R[x,x^{-1}]^{\bullet}$- и $R[x]^{\bullet}$-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

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

Эти операции задают структуры левого $\mathcal{L}R^{\langle 1\rangle}$-модуля и левого $\mathcal{L}R^{\langle 1\rangle\bullet}$-модуля на множестве $\mathcal{L}M^{\langle 1\rangle}$. Аналогично определяется покоординатное произведение бипоследовательностей над R и M и структура левого $\mathcal{L}R_{\mathrm{bi}}^{\langle 1\rangle\bullet}$-модуля на $\mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle}$.

Зададим отображение $\rho\colon \mathcal{L}M^{\langle 1\rangle}\to\mathcal{L}R^{\langle 1\rangle}\otimes\mathcal{L}M^{\langle 1\rangle}$ следующим образом: если $u\in L_M(F)$, $\deg F(x)=m$, то

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

Точно так же отображение $\rho\colon \mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle}\to\mathcal{L}R_{\mathrm{bi}}^{\langle 1\rangle}\otimes\mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle}$ задаётся для бипоследовательностей.

Теорема 9. *Модули $\mathcal{L}M^{\langle 1\rangle}$, $\mathcal{L}M^{\langle 1\rangle}$, $\mathcal{L}M_{\mathrm{bi}}^{\langle 1\rangle}$, $\mathcal{L}M_{\mathrm{rev}}^{\langle 1\rangle}$ являются левыми хопфовыми соответственно $\mathcal{L}R^{\langle 1\rangle}$-, $\mathcal{L}R^{\langle 1\rangle\bullet}$-, $\mathcal{L}R_{\mathrm{bi}}^{\langle 1\rangle\bullet}$-, $\mathcal{L}R_{\mathrm{rev}}^{\langle 1\rangle\bullet}$-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

$$u=\sum_{\alpha\in A}u_\alpha m_\alpha, \tag{35}$$

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 $u(i)=\sum\limits_{\alpha}c_{i\alpha}m_\alpha$, $0\leqslant i\leqslant m-1$, 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 $(c_{0\alpha},\ldots,c_{m-1,\alpha})$, $\alpha\in A$. Тогда лишь конечное число u_α отличны от 0 и $\sum\limits_{\alpha}u_\alpha m_\alpha$ — последовательность из $L_M(F)$, начальный вектор которой совпадает с $u(\overline{0,m-1})$. 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. Имеем

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

Так как в силу теоремы 6 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, т. е. 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 $u = \sum\limits_\alpha v_\alpha m_\alpha$, где $v_\alpha \in L_R(G)$ и лишь конечное число v_α отличны от 0. При этом $u_\alpha, v_\alpha \in L_R(FG)$. Пользуясь следствием 4 (т. е. фактически корректностью определения коумножения Δ формулой из утверждения 3), получаем

$$\sum_{t=0}^{m-1} e_t^F \otimes x^t u = \sum_{t=0}^{m-1} e_t^F \otimes x^t \sum_\alpha u_\alpha m_\alpha = \sum_\alpha \biggl(\sum_{t=0}^{m-1} e_t^F \otimes x^t u_\alpha \biggr) m_\alpha =$$
$$= \sum_\alpha \biggl(\sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t u_\alpha \biggr) m_\alpha = \sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t \sum_\alpha u_\alpha m_\alpha = \sum_{t=0}^{m+n-1} e_t^{FG} \otimes x^t u,$$

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, т. е. выполнены условия (31). Пусть $u \in L_M(F)$. Тогда

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

Чтобы доказать равенство, достаточно проверить, что для любого $s \in \overline{0, m-1}$

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

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):

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

Остаётся проверить условие (33). Так как в этом условии задействовано умножение последовательностей, то доказательства существенно различаются для конволюции и покоординатного 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 $i, j \geqslant 0$

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

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 покоординатно. 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 $i, j \geqslant 0$

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

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 бипоследовательностей все доказательства сохраняются. □

7. Обобщение на полилинейные рекуррентные последовательности

Произвольная функция $u\colon \mathbb{N}_0^k \to M$ 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 $M^{\langle k\rangle}$.

k-последовательность u называется *k-линейной рекуррентной последовательностью* (k-ЛРП) над модулем M, если существуют унитарные многочлены $F_1(x), \ldots, F_k(x) \in R[x]$, такие что для любого $s \in \overline{1,k}$ и для любых $i_1, \ldots, i_{s-1}, i_{s+1}, \ldots, i_k \in \mathbb{N}_0$ последовательность

$$v(i) = u(i_1, \ldots, i_{s-1}, i, i_{s+1}, \ldots, i_k), \quad i \geqslant 0,$$

есть ЛРП над R-модулем M с характеристическим многочленом $F_s(x)$. В случае $k = 1$ определение 1-ЛРП совпадает с определением ЛРП. Многочлены $F_1(x_1), \ldots, F_k(x_k)$ из кольца $R[\boldsymbol{x}] = R[x_1, \ldots, x_k]$ многочленов от k переменных называются *элементарными характеристическими многочленами k-ЛРП u*. Множество всех k-ЛРП над M обозначим $\mathcal{L}M^{\langle k\rangle}$, а множество k-ЛРП с элементарными характеристическими многочленами $F_1(x_1), \ldots, F_k(x_k)$ будем обозначать $L_M(\boldsymbol{F}) = L_M(F_1, \ldots, F_k)$. Назовём k-ЛРП *u реверсивной*, если $u \in L_M(\boldsymbol{F})$, где каждый из многочленов $F_1(x), \ldots, F_k(x)$ реверсивен. Множество реверсивных k-ЛРП над M обозначим $\mathcal{L}M_{\mathrm{rev}}^{\langle k\rangle}$.

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 $F_2(x)$.

Обозначим $\boldsymbol{x}^{\boldsymbol{s}} = x_1^{s_1} \ldots x_k^{s_k}$. *Сдвигом* k-последовательности $u \in M^{\langle k\rangle}$ на вектор $\boldsymbol{s}$ называется k-последовательность $\boldsymbol{x}^{\boldsymbol{s}} u$ со знаками $\boldsymbol{x}^{\boldsymbol{s}} u(\boldsymbol{i}) = u(\boldsymbol{s} + \boldsymbol{i})$, $\boldsymbol{i} \in \mathbb{N}_0^k$. Определим умножение многочлена $F(\boldsymbol{x}) = \sum\limits_{\boldsymbol{s}} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}} \in R[\boldsymbol{x}]$ на k-последовательность u правилом

$$F(\boldsymbol{x})u = \sum_{\boldsymbol{s}} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}} u, \quad \text{т. е. } (F(\boldsymbol{x})u)(\boldsymbol{i}) = \sum_{\boldsymbol{s}} c_{\boldsymbol{s}} u(\boldsymbol{i}+\boldsymbol{s}), \quad \boldsymbol{i} \in \mathbb{N}_0^k. \tag{36}$$

Тогда $M^{\langle k \rangle}$ превращается в левый $R[\boldsymbol{x}]$-модуль. Идеал

$$\mathrm{An}(u) = \{F(\boldsymbol{x}) \in R[\boldsymbol{x}]\colon\ F(\boldsymbol{x})u = 0\}$$

назовём *аннулятором* k-последовательности u. Тогда u есть k-ЛРП над M в том и только в том случае, когда идеал $\mathrm{An}(u)$ *унитарен*, т. е. содержит набор унитарных многочленов $F_1(x_1), \ldots, F_k(x_k)$.

Каждой k-последовательности $u \in \mathcal{L}R^{\langle k \rangle}$ над кольцом R сопоставим отображение

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

Это сопоставление взаимно-однозначно и индуцирует на $R[\boldsymbol{x}]^*$ структуру левого $R[\boldsymbol{x}]$-модуля по правилу

$$F(\boldsymbol{x})\hat{u} = \hat{u}\hat{F}, \quad \text{где } \hat{F}\colon R[\boldsymbol{x}] \to R[\boldsymbol{x}],\ \hat{F}(G) = GF, \text{ — гомотетия.}$$

При этом $F(\boldsymbol{x}) \in \mathrm{An}(u) \iff F(\boldsymbol{x})R[\boldsymbol{x}] \subseteq \mathrm{Ker}\,\hat{u}$.

Произвольная функция $u\colon \mathbb{Z}^k \to M$ называется *k-бипоследовательностью* над M. Пусть $R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ — алгебра многочленов Лорана от k переменных из примера 2. Введём на множестве k-бипоследовательностей $M_{\mathrm{bi}}^{\langle k \rangle}$ структуру левого $R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$-модуля, определив умножение многочлена $F(\boldsymbol{x}) = \sum_{\boldsymbol{s} \in \mathbb{Z}^k} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}} \in R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ на k-бипоследовательность u правилом (36). Идеал $\mathrm{An}(u) = \{F(\boldsymbol{x}) \in R[\boldsymbol{x}, \boldsymbol{x}^{-1}]\colon\ F(\boldsymbol{x})u = 0\}$ называется *аннулятором* k-бипоследовательности u.

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

Если $u \in L_M(F_1, \ldots, F_k)$, $\deg F_s = m_s$, то множество

$$\Pi = \Pi(\boldsymbol{m}) = \overline{0, m_1 - 1} \times \ldots \times \overline{0, m_k - 1}$$

называется *начальным параллелепипедом* k-ЛРП u. Пусть $\Pi = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_m\}$, где $m = |\Pi| = m_1 \ldots m_k$. Тогда вектор $u[\Pi] = (u(\boldsymbol{i}_1), \ldots, u(\boldsymbol{i}_m)) \in M^\Pi = M^m$ назовём *начальным вектором* k-ЛРП u. Для каждого $\delta[\Pi] \in M^\Pi$ существует единственная k-ЛРП $u \in L_M(\boldsymbol{F})$ с начальным вектором $u[\Pi] = \delta[\Pi]$. Действительно, например, в случае $k = 2$ для получения u продолжим $\delta[\Pi]$ до m_2 последовательностей $u(i, j)$, $i \geqslant 0$, $0 \leqslant j < m_2$, из $L_M(F_1)$ и расположим их в первых m_2 строках бесконечного массива, а затем каждый начальный вектор $u(i, j)$, $0 \leqslant j < m_2$, продолжим до последовательности $u(i, j)$, $j \geqslant 0$, расположенной в i-м столбце массива, $i \geqslant 0$. Из сказанного следует, что $L_M(\boldsymbol{F})$ есть свободный R-модуль ранга m. Аналогичное утверждение верно для бипоследовательностей из $L_M^{\mathrm{bi}}(\boldsymbol{F})$. Для $\boldsymbol{t} \in \Pi$ через $e_{\boldsymbol{t}}^{\boldsymbol{F}}$ будем обозначать k-(би)последовательность из $L_R(\boldsymbol{F})$ или $L_R^{\mathrm{bi}}(\boldsymbol{F})$ с начальным вектором $e_{\boldsymbol{t}}^{\boldsymbol{F}}(\boldsymbol{t}) = 1$, $e_{\boldsymbol{t}}^{\boldsymbol{F}}(\boldsymbol{i}) = 0$ при $\boldsymbol{i} \in \Pi(\boldsymbol{m}) \setminus \{\boldsymbol{t}\}$. (Би)последовательность $e^{\boldsymbol{F}} = e_{\boldsymbol{m-1}}^{\boldsymbol{F}}$ назовём *импульсной (би)последовательностью* семейств $L_R(\boldsymbol{F})$ и $L_R^{\mathrm{bi}}(\boldsymbol{F})$.

Реверсом k-бипоследовательности u назовём k-бипоследовательность $u^*\colon \mathbb{Z}^k \to M$, определяемую равенствами $u^*(\boldsymbol{i}) = u(-\boldsymbol{i})$, $\boldsymbol{i} \in \mathbb{Z}^k$. Каждую реверсивную k-ЛРП $u \in L_M(\boldsymbol{F})$ можно единственным образом продолжить до k-ЛРБ $u \in L_M^{\mathrm{bi}}(\boldsymbol{F})$ с тем же начальным вектором $u[\Pi]$. Отождествляя реверсивную k-ЛРП и указанную k-ЛРБ, получим, что

$$\mathcal{L}M_{\mathrm{rev}}^{\langle k\rangle} \equiv \mathcal{L}M_{\mathrm{bi}}^{\langle k\rangle}.$$

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

Каждой k-бипоследовательности $u \in M_{\mathrm{bi}}^{\langle k\rangle}$ сопоставим отображение

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

Утверждение 10. *Пусть A — алгебра многочленов $R[\boldsymbol{x}]$ или $R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ над коммутативным кольцом R с единицей, K — R-подмодуль в A. Тогда условия* (а)—(г) *утверждения* 1 *эквивалентны. Справедливы равенства*

$$R[\boldsymbol{x}]^* \equiv R^{\langle k\rangle}, \quad R[\boldsymbol{x}]^\circ \equiv \mathcal{L}R^{\langle k\rangle},$$
$$R[\boldsymbol{x}, \boldsymbol{x}^{-1}]^* \equiv R_{\mathrm{bi}}^{\langle k\rangle}, \quad R[\boldsymbol{x}, \boldsymbol{x}^{-1}]^\circ \equiv \mathcal{L}R_{\mathrm{bi}}^{\langle k\rangle} \equiv \mathcal{L}R_{\mathrm{rev}}^{\langle k\rangle}.$$

Доказательство. Импликации (а $\Rightarrow$ б $\Rightarrow$ в) очевидны. Пусть $A = R[\boldsymbol{x}]$. Тогда импликация (г $\Rightarrow$ а) также очевидна. Докажем импликацию (в $\Rightarrow$ г) (доказательство отличается от доказательства утверждения 1 и аналогично доказательству утверждения 1.13 из [11]). Пусть R-модуль $R[\boldsymbol{x}]/I$ порождается элементами $\bar{F}_1, \ldots, \bar{F}_n$, где $\bar{F} = F + I$. Тогда $\bar{x}_1 \bar{F}_j(\boldsymbol{x}) = \sum\limits_i a_{ij} \bar{F}_i$ для некоторых $a_{ij} \in R$, $1 \leqslant i, j \leqslant n$. Рассмотрим матрицу $A = (a_{ij}) \in R_n$. Если $c = (c_1, \ldots, c_n)$ — вектор коэффициентов в разложении элемента $\bar{G} \in R[\boldsymbol{x}]/I$ в системе образующих $\bar{F}_1, \ldots, \bar{F}_n$, то cA — вектор коэффициентов в разложении элемента $\bar{x}_1 \bar{G}$. Пусть c — вектор коэффициентов в разложении элемента $\bar{1}$. Тогда последовательность векторов $c, cA, cA^2, \ldots$, являющихся векторами коэффициентов в разложении элементов $\bar{1}, \bar{x}_1, \bar{x}_1^2, \ldots$, аннулируется характеристическим многочленом $\chi_A(x)$ матрицы A. Следовательно, $\bar{\chi}_A(x_1) = 0$, т. е. $\chi_A(x_1) \in I$. Таким образом, I содержит унитарный многочлен от переменной x_1. Аналогично доказывается, что I содержит унитарный многочлен от x_s, $1 \leqslant s \leqslant k$, т. е. I унитарен.

Пусть теперь $A = R[\boldsymbol{x}, \boldsymbol{x}^{-1}]$.

(в $\Rightarrow$ г) Пусть R-модуль $R[\boldsymbol{x}, x^{-1}]/I$ порождается элементами $\bar{F}_1, \ldots, \bar{F}_n$, где $\bar{F} = F + I$. Рассуждая как и выше, построим матрицу A и унитарный многочлен $\chi_A(x_1) \in I$. Достаточно доказать, что многочлен $\chi_A(x)$ реверсивен, т. е. что матрица A обратима. Пусть $\bar{x}_1^{-1} \bar{F}_j(\boldsymbol{x}) = \sum\limits_i b_{ij} \bar{F}_i$, $b_{ij} \in R$, $1 \leqslant i, j \leqslant n$, и пусть

$B = (b_{ij})$. Равенства $x_1^{-1}x_1F_j(\boldsymbol{x}) = F_j(\boldsymbol{x})$, $1 \leqslant j \leqslant n$, показывают, что $AB = E$. Поэтому матрица A обратима.

(г $\Rightarrow$ а) Пусть выполняется условие (г) и $m_s = \deg F_s(x)$. Докажем, что $R[\boldsymbol{x}, \boldsymbol{x}^{-1}]/I$ — конечно порождённый свободный R-модуль с базисом $\boldsymbol{x}^{\boldsymbol{i}} + I$, $\boldsymbol{i} \in \Pi = \Pi(\boldsymbol{m})$. Действительно, очевидно, что $\boldsymbol{x}^{\boldsymbol{i}} + I$, $\boldsymbol{i} \in \Pi$ — система образующих. Если эти элементы линейно зависимы над R, то идеал I содержит ненулевой многочлен вида $H(\boldsymbol{x}) = \sum\limits_{\boldsymbol{i}\in\Pi} c_{\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}$. Тогда $H(\boldsymbol{x})$ должен аннулировать импульсную k-бипоследовательность семейства $L_R^{\mathrm{bi}}(\boldsymbol{F})$, что невозможно. $\square$

Отметим, что если дуальные алгебры рассматривать относительно модуля M, т. е. положить $A^* = \mathrm{Hom}_R(A, M)$ и A° определить так же, как в (7), то из утверждения 10 вытекают равенства

$$R[\boldsymbol{x}]^* \equiv M^{\langle k\rangle}, \quad R[\boldsymbol{x}]^\circ \equiv \mathcal{L}M^{\langle k\rangle},$$
$$R[\boldsymbol{x}, \boldsymbol{x}^{-1}]^* \equiv M_{\mathrm{bi}}^{\langle k\rangle}, \quad R[\boldsymbol{x}, \boldsymbol{x}^{-1}]^\circ \equiv \mathcal{L}M_{\mathrm{bi}}^{\langle k\rangle} \equiv \mathcal{L}M_{\mathrm{rev}}^{\langle k\rangle}.$$

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

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

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

$$\begin{aligned} (u * v)(\boldsymbol{i}) &= \sum_{\boldsymbol{0}\leqslant\boldsymbol{j}\leqslant\boldsymbol{i}} \binom{\boldsymbol{i}}{\boldsymbol{j}} u(\boldsymbol{j})v(\boldsymbol{i} - \boldsymbol{j}), \\ (uv)(\boldsymbol{i}) &= u(\boldsymbol{i})v(\boldsymbol{i}), \\ e_*(\boldsymbol{i}) &= \delta_{\boldsymbol{0}\boldsymbol{i}}, \\ e^\bullet(\boldsymbol{i}) &= 1, \\ \varepsilon(u) &= u(\boldsymbol{0}), \\ S(u)(\boldsymbol{i}) &= (-\boldsymbol{1})^{\boldsymbol{i}}u(\boldsymbol{i}), \\ S^\bullet(u)(\boldsymbol{i}) &= u(-\boldsymbol{i}), \end{aligned} \tag{38}$$

где $\binom{\boldsymbol{i}}{\boldsymbol{j}} = \binom{i_1}{j_1}\ldots\binom{i_k}{j_k}$, $\delta_{\boldsymbol{0}\boldsymbol{i}}$ — символ Кронекера, $(-\boldsymbol{1})^{\boldsymbol{i}} = (-1)^{i_1+\ldots+i_k}$ и отношение частичного порядка $\leqslant$ на множестве $\mathbb{Z}^k$ задаётся следующим образом: $\boldsymbol{j} \leqslant \boldsymbol{i} \iff j_1 \leqslant i_1, \ldots, j_k \leqslant i_k$. Коумножение Δu определяется условием

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

или в сокращённой записи

$$\Delta u(\boldsymbol{i} \otimes \boldsymbol{j}) = u(\boldsymbol{i} + \boldsymbol{j}). \tag{39}$$

Если $u \in L_R(\boldsymbol{F})$ или $u \in L_R^{\text{bi}}(\boldsymbol{F})$, то верно равенство

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

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

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

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

$$R[x]^\circ \otimes \ldots \otimes R[x]^\circ \to R[\boldsymbol{x}]^\circ, \quad R[x, x^{-1}]^\circ \otimes \ldots \otimes R[x, x^{-1}]^\circ \to R[\boldsymbol{x}, \boldsymbol{x}^{-1}]^\circ,$$

при которых элементу $u_1 \otimes \ldots \otimes u_k$ сопоставляется k-(би)последовательность u со знаками $u(\boldsymbol{i}) = u_1(i_1) \ldots u_k(i_k)$, являются изоморфизмами между k-ми тензорными степенями биалгебр(20) и биалгебрами (37).

Мы видим, что операции в биалгебрах 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, утверждения 7, требующего дополнительного рассмотрения). Перечислим основные из них.

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

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

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

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

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

Биномиальная k-последовательность $\boldsymbol{a}^{[\boldsymbol{n}]}$ реверсивна тогда и только тогда, когда $\boldsymbol{a} \in U(R)^k$. В этом случае соотношения (40) определяют продолжение $\boldsymbol{a}^{[\boldsymbol{n}]}$ до биномиальной бипоследовательности $\boldsymbol{a}^{[\boldsymbol{n}]} \colon \mathbb{Z}^k \to R$. Легко увидеть, что $\boldsymbol{a}^{[\boldsymbol{n}]}$ есть импульсная (би)последовательность семейства $L_R((\boldsymbol{x}-\boldsymbol{a})^{\boldsymbol{n}+\boldsymbol{1}}) = L_R((x_1-a_1)^{n_1+1},\ldots,(x_k-a_k)^{n_k+1})$. Биномиальная (би)последовательность порядка $\boldsymbol{0}$ — это геометрическая прогрессия $\boldsymbol{a}^{[\boldsymbol{0}]}(\boldsymbol{i}) = \boldsymbol{a}^{\boldsymbol{i}}$. Биномиальные (би)последовательности $\boldsymbol{a}^{[\boldsymbol{n}]}$, $\boldsymbol{n}\in\mathbb{N}_0^k$, удовлетворяют соотношению

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

Естественные определения конволюции и покоординатного произведения k-ЛРП над кольцом R и k-ЛРП над модулем M задают структуры левого $\mathcal{L}R^{\langle k\rangle}$- и $\mathcal{L}R^{\langle k\rangle\bullet}$-модулей на $\mathcal{L}M^{\langle k\rangle}$. Аналогично покоординатное произведение ЛРБ над R и над M задаёт структуру левого $\mathcal{L}R_{\mathrm{bi}}^{\langle k\rangle\bullet}$-модуля на $\mathcal{L}M_{\mathrm{bi}}^{\langle k\rangle}$. Определим отображение $\rho\colon \mathcal{L}M^{\langle k\rangle}\to\mathcal{L}R^{\langle k\rangle}\otimes\mathcal{L}M^{\langle k\rangle}$ следующим образом: если $u\in L_M(F_1,\ldots,F_k)$, $\deg F_s(x)=m_s$, то

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

Для бипоследовательностей ρ определяется аналогично. Тогда модули $\mathcal{L}M^{\langle k\rangle}$, $\mathcal{L}M^{\langle k\rangle}$, $\mathcal{L}M_{\mathrm{bi}}^{\langle k\rangle}$, $\mathcal{L}M_{\mathrm{rev}}^{\langle k\rangle}$ являются левыми хопфовыми соответственно $\mathcal{L}R^{\langle k\rangle}$-, $\mathcal{L}R^{\langle k\rangle\bullet}$-, $\mathcal{L}R_{\mathrm{bi}}^{\langle k\rangle\bullet}$-, $\mathcal{L}R_{\mathrm{rev}}^{\langle k\rangle\bullet}$-модулями относительно структурного отображения ρ.

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

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

Если $u\in L_M(F_1,\ldots,F_k)$, $\deg F_s(x)=m_s$, $F_s^{(*)}(x)=x^{m_s}F_s(1/x)$, то $F_s^{(*)}(0)=1$ и легко увидеть, что $F_1^{(*)}(x_1)\ldots F_k^{(*)}(x_k)u(\boldsymbol{x}) = H(\boldsymbol{x})$, где $H(\boldsymbol{x})$ — многочлен из $M[\boldsymbol{x}]$, степень которого по каждой переменной x_s меньше m_s. С другой стороны, если $G_1(x),\ldots,G_k(x)\in R[x]$ — такие многочлены, что $G_s(0)=1$, то $G_s(x_s)$ обратим как элемент кольца $R[[\boldsymbol{x}]]$ и определён ряд $u(\boldsymbol{x}) = 1/(G_1(x_1)\ldots G_k(x_k)) = \sum_{\boldsymbol{i}} u(\boldsymbol{i})\boldsymbol{x}^{\boldsymbol{i}}\in R[[\boldsymbol{x}]]$, коэффициенты которого образуют k-ЛРП $u=(u(\boldsymbol{i}))$ из $L_R(G_1^{(*)},\ldots,G_k^{(*)})$. Отождествляя k-последовательность u с её производящей функцией $u(x)$, получим, что

$$\mathcal{L}M^{\langle k\rangle}\equiv M_{\mathrm{rat}}[[\boldsymbol{x}]],$$

где $M_{\mathrm{rat}}[[\boldsymbol{x}]]$ — множество таких рядов $a(\boldsymbol{x})\in M[[\boldsymbol{x}]]$, что

$$G_1(x_1)\ldots G_k(x_k)a(\boldsymbol{x})\in M[\boldsymbol{x}]$$

для некоторых многочленов $G_1(x),\ldots,G_k(x)\in R[x]$, удовлетворяющих условию $G_s(0)=1$.

Каждая k-ЛРП $u\in L_M(\boldsymbol{F})$ однозначно представляется в виде $u=\Phi(\boldsymbol{x})e^{\boldsymbol{F}}$, где $\Phi(\boldsymbol{x})\in M[\boldsymbol{x}]$ — многочлен, степень которого по x_s меньше m_s, называемый *генератором* k-ЛРП u относительно элементарных характеристических многочленов $F_1, \ldots, F_k$. Справедлива формула

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

где $\Phi^{(*)}(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{m}-\boldsymbol{1}} \Phi(\boldsymbol{x}^{-1}) = x_1^{m_1-1} \ldots x_k^{m_k-1} \Phi(x_1^{-1}, \ldots, x_k^{-1})$, или

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

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

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

где $\boldsymbol{i}! = i_1! \ldots i_k!$. Отображение $(\mathcal{L}R^{\langle k \rangle}, *, e_*) \to (R[[\boldsymbol{x}]], \cdot, 1)$, $u \to U(\boldsymbol{x})$, является мономорфизмом алгебр, т. е. конволюции $u * v$ последовательностей отвечает умножение по Коши экспоненциальных производящих функций. Так как

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

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

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

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

$$L_R(I) = \{u \in \mathcal{L}M^{\langle k \rangle} : \; F(\boldsymbol{x}) u = 0 \text{ для всех } F(\boldsymbol{x}) \in I\}$$

можно рассматривать как множество решений системы линейных дифференциальных уравнений $F(\frac{d}{d\boldsymbol{x}}) U(\boldsymbol{x}) = 0$, $F \in I$.

Справедливо также утверждение, что k-(би)последовательность является представляющей функцией на полугруппе $G = \mathbb{N}_0^k$ (соответственно $G = \mathbb{Z}^k$) со значениями в M тогда и только тогда, когда она является k-линейной рекуррентной (би)последовательностью над модулем M. Таким образом, $\mathcal{R}(M^{\mathbb{N}_0^k}) = \mathcal{L}M^{\langle k \rangle}$ и $\mathcal{R}(M^{\mathbb{Z}^k}) = \mathcal{L}M_{\mathrm{bi}}^{\langle k \rangle}$.

Литература

[1] Артамонов В. А. Строение алгебр Хопфа // Итоги науки и техники. Алгебра, геометрия, топология. Т. 29. — М.: ВИНИТИ, 1991. — С. 3—63.

[2] Бахтурин Ю. А. Основные структуры современной алгебры. — М.: Наука, 1990.

[3] Куракин В. Л. Конволюция линейных рекуррентных последовательностей // Успехи мат. наук. — 1993. — Т. 48, № 4. — С. 235—236.

[4] Куракин В. Л. Строение алгебр Хопфа линейных рекуррентных последовательностей // Успехи мат. наук. — 1993. — Т. 48, № 5. — С. 177—178.

[5] Куракин В. Л. Алгебры Хопфа линейных рекуррентных последовательностей над коммутативными кольцами // Труды Вторых математических чтений МГСУ. Нахабино, 26 января—2 февраля 1994 г. — М., 1994. — С. 67—69.

[6] Куракин В. Л. Алгебра Хопфа, дуальная к алгебре многочленов над коммутативным кольцом. — Подготовлено для опубликования.

[7] Abuhlail J. Y., Gómez-Torrecillas J., Wisbauer R. Dual coalgebras of algebras over commutative rings // J. Pure and Appl. Algebra. — 2000. — Vol. 153. — P. 107—120.

[8] Cerlienco L., Piras F. On the continuous dual of a polynomial bialgebra // Comm. Algebra. — 1991. — Vol. 19, no. 10. — P. 2707—2727.

[9] Chin W., Goldman J. Bialgebras of lineary recursive sequences // Comm. Algebra. — 1993. — Vol. 21, no. 11. — P. 3935—3952.

[10] Haukkanen P. On a convolution of linear recurring sequences over finite fields. I, II // J. Algebra. — 1992. — Vol. 149, no. 1. — P. 179—182; 1994. — Vol. 164, no. 2. — P. 542—544.

[11] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // Journal of Mathematical Sciences. — 1995. — Vol. 76, no. 6. — P. 2793—2915.

[12] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N. Linear and polylinear recurring sequences over abelian groups and modules // Journal of Mathematical Sciences. — 2000. — Vol. 102, no. 6. — P. 4598—4627.

[13] Peterson B., Taft E. Y. The Hopf algebra of linear recursive sequences // Aequat. Math. — 1980. — Vol. 20. — P. 1—17.

[14] Snapper E. Completely primary rings, I // Ann. Math. — 1950. — Vol. 52, no. 3. — P. 666—693.

[15] Sweedler M. F. Hopf algebras. — New York: Benjamin, 1969.

[16] Zierler N., Mills W. H. Products of linear recurring sequences // J. Algebra. — 1973. — Vol. 27, no. 1. — P. 147—157.