Современная математика и ее приложения. Том 14 (2004). С. 3–10

УДК 512.554.3

ПОЛУОБЛАСТИ И МЕТАБЕЛЕВО ПРОИЗВЕДЕНИЕ МЕТАБЕЛЕВЫХ АЛГЕБР ЛИ

© 2004 г. **Э. Ю. ДАНИЯРОВА, И. В. КАЗАЧКОВ, В. Н. РЕМЕСЛЕННИКОВ**

Аннотация. Для категории метабелевых алгебр Ли введены понятия полуобласти и строгой полуобласти и исследованы их свойства.

СОДЕРЖАНИЕ

1. Введение

Данная статья написана в рамках проекта по построению алгебраической геометрии над метабелевыми алгебрами Ли, начатого работами авторов [3–5].

Пусть A — метабелева алгебра Ли над полем k, $S(x) = 0$ — система уравнений от набора неизвестных $X = \{x_1, \ldots, x_n\}$ над алгеброй A, $V(S)$ — алгебраическое множество из A^n, определенное системой S. Анализ доказательств теорем о структуре $V(S)$ и его координатной алгебры $\Gamma(S)$ из [4] показывает, что необходимые вычисления проводятся в алгебре $A[X] = A * F(X)$, где $F(X)$ — свободная алгебра Ли, а $*$ — знак метабелева произведения. Это обстоятельство объясняет внимание к проблеме исследования структуры метабелева произведения метабелевых алгебр Ли. Решение проблемы дано теоремами 1, 2 и 4.

Понятия *области* в категории групп (групп не имеющих делителей нуля) было введено в [7], где показана важность этого понятия при установлении критериев неприводимости алгебраических множеств. Любая метабелева алгебра Ли (а также всякая метабелева группа), имеющая неединичные абелевы идеалы (соответственно, подгруппы) имеет делители нуля, поэтому в категории метабелевых алгебр Ли указанное понятие не работает (коммутант метабелевой алгебр Ли является абелевым идеалом). Для этой категории мы вводим понятие *полуобласти* и *строгой полуобласти* и исследуем их свойства с тем, чтобы в дальнейшем применить полученные результаты в алгебраической геометрии.

2. Предварительные сведения

Ниже приведен краткий обзор необходимых сведений об алгебрах Ли (см. [2]).

Напомним, что A называется метабелевой алгеброй Ли над полем k, если A — алгебра Ли над полем k и, кроме того, на A выполнена универсальная аксиома

$$(a \circ b) \circ (c \circ d) = 0.$$

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 02-01-00192) и гранта «Университеты России».

ISSN 1512–1712

Через $a \circ b$ или ab будем обозначать произведение элементов алгебры A. Запись $a_1a_2a_3 \dots a_n$ означает *левонормированное произведение* (или *левонормированное слово*, или *моном длины*, или *степени* n) элементов $a_1, a_2, a_3, \dots, a_n$, т.е.

$$(\dots((a_1 \circ a_2) \circ a_3) \circ \dots) \circ a_n.$$

Как известно (см. [1]), произвольный моном длины n от букв $a_1, \dots, a_n$ в алгебре Ли может быть представлен в виде линейной комбинации левонормированных мономов длины n от этих же букв.

Пусть A — алгебра Ли над полем k. Через $\langle x \rangle$ будем обозначать главный идеал алгебры Ли A, порожденный элементом $x \in A$. Как известно (см. [2]), идеал $\langle x \rangle$ является линейной оболочкой над полем k левонормированных слов алгебры A, начинающихся с буквы x:

$$x,\ xa_1,\ xb_1b_2,\ \dots,\ xc_1c_2 \cdots c_n,\ \dots.$$

Идеал, порожденный множеством $\{a \circ b \mid a, b \in A\}$, называется *коммутантом* алгебры A и обозначается A^2. *Радикалом Фиттинга* $\mathrm{Fit}(A)$ алгебры Ли A называется идеал, порожденный множеством, состоящим из элементов всех нильпотентных идеалов алгебры A. Известна следующая характеризация радикала Фиттинга: элемент $x \in A$ принадлежит $\mathrm{Fit}(A)$ тогда и только тогда, когда идеал $\langle x \rangle$ нильпотентен (см. [3]).

Пусть F — свободная алгебра в многообразии $\mathscr{A}^2$ всех метабелевых алгебр Ли. Пусть $\{a_\alpha \mid \alpha \in \Lambda\}$ — свободная база алгебры F. Предположим, что множество Λ вполне упорядочено. Тогда левонормированные мономы $a_{i_1}a_{i_2} \dots a_{i_m}$, в которых $i_1 > i_2 \leqslant i_3 \leqslant \dots \leqslant i_m$, будем называть *нормированными* В [1] доказано, что нормированные слова составляют линейный базис алгебры F.

Пусть A — произвольная метабелева алгебра Ли над полем k. Тогда на коммутанте A^2 имеется структура модуля над кольцом коммутативных многочленов $R = k[X]$, где X — линейная база векторного пространства A/A^2 (см. [3]).

3. Метабелевы произведения метабелевых алгебр Ли

Пусть A и B — ненулевые метабелевы k алгебры Ли. Считаем, что поле k фиксировано, поэтому в дальнейшем будем подразумевать под $\mathscr{A}^2$ многообразие всех метабелевых k-алгебр Ли. Через $A * B$ обозначим произведение алгебр A и B в многообразии $\mathscr{A}^2$. Напомним определение алгебры $A * B$.

Определение 1. Пусть

$$A = \langle z_i, i \in I_A \mid R_A \rangle_{\mathscr{A}^2}, \quad B = \langle z_i, i \in I_B \mid R_B \rangle_{\mathscr{A}^2}$$

— представления алгебр A и B в многообразии $\mathscr{A}^2$. Предположим, что $I_A \cap I_B = \emptyset$. Тогда алгебра $A * B$ в многообразии $\mathscr{A}^2$ определяется следующим образом:

$$A * B = \langle z_i, i \in I_A \cup I_B \mid R_A \cup R_B \rangle_{\mathscr{A}^2}.$$

Приведем также категорное определение алгебры $A * B$, эквивалентное определению 1.

Определение 2 (категорное определение)**.** Метабелева алгебра $C \in \mathscr{A}^2$ называется метабелевым произведением метабелевых алгебр A и B если выполнены два следующих условия:

1) существуют вложения $i_A : A \to C$ и $i_B : B \to C$, причем алгебра C порождается образами $i_A(A)$ и $i_B(B)$: $C = \langle i_A(A), i_B(B) \rangle_{\mathscr{A}^2}$;
2) для любой метабелевой алгебры H над полем k и любой пары вложений $\psi_A : A \to H$ и $\psi_B : B \to H$ существует гомоморфизм $\phi : C \to H$ такой, что $\phi i_A = \psi_A$ и $\phi i_B = \psi_B$.

В данном разделе мы изучим структуру алгебры $A * B$ и покажем, что $\mathrm{Fit}(A * B) = (A * B)^2$.

Пусть $\overline{A}$ и $\overline{B}$ — векторные пространства над полем k: $\overline{A} = A/A^2$ и $\overline{B} = B/B^2$. Обозначим через $X = \{x_i \mid i \in I\}$ и $Y = \{y_j \mid j \in J\}$ линейные базисы пространств $\overline{A}$ и $\overline{B}$ соответственно. Символами элементов из множеств X и Y мы также будем обозначать их прообразы в алгебрах A

и B. Будем считать, что множества I и J вполне упорядочены. Как отмечено выше, на коммутанте A^2 имеется структура модуля над кольцом многочленов $R_X = k[X]$, соответственно на B^2 имеется структура модуля над кольцом $R_Y = k[Y]$.

Так как векторное пространство $A * B/(AB)^2$ над полем k порождается образами элементов из $X \cup Y$, то коммутант $(A * B)^2$ алгебры $A * B$ является модулем над кольцом многочленов $R_{X\cup Y} = k[X \cup Y]$.

Чтобы определить модульную структуру алгебры $A * B$, поступим следующим образом.

1. Определим тройку $R_{X\cup Y}$-модулей M_0, M_1 и M_2. По этим модулям построим $R_{X\cup Y}$-модуль M.
2. По модулю M построим метабелеву алгебру Ли C и докажем, что C изоморфна $A * B$. Этот изоморфизм и даст достаточно хорошее структурное описание алгебры $A * B$.

Расширим модули A^2 и B^2 до модулей над кольцом $R_{X\cup Y}$, полагая

$$M_1 = A^2 \otimes_{R_X} R_{X\cup Y}, \quad M_2 = B^2 \otimes_{R_Y} R_{X\cup Y},$$

где $\otimes$ — знак тензорного умножения. Кроме того, через M_0 обозначим $R_{X\cup Y}$-модуль, изоморфный идеалу кольца $R_{X\cup Y}$, порожденному множеством $\{x_i y_j \mid i \in I,\ j \in J\}$. В частности, модуль M_0 не имеет кручения. Определим $R_{X\cup Y}$-модуль M с помощью порождающих и определяющих соотношений. Пусть

$$A^2 = \langle Z_1 | R_1 \rangle, \quad B^2 = \langle Z_2 | R_2 \rangle, \quad Z_1 \cap Z_2 = \emptyset,$$

— задания R_X-модуля A^2 и R_Y-модуля B^2 с помощью порождающих и соотношений. Положим $XY = \{x_i y_j \mid i \in I,\ j \in J\}$, $Z = Z_1 \cup Z_2$ и

$$M = \langle XY \cup Z \mid R_1 \cup R_2 \cup S \rangle, \tag{1}$$

где

$$S = \begin{cases} (x_i y_{j_1}) \cdot y_{j_2} = (x_i y_{j_2}) \cdot y_{j_1} + (y_{j_2} y_{j_1}) \cdot x_i, & j_1 > j_2, \\ (x_{i_1} y_j) \cdot x_{i_2} = (x_{i_2} y_j) \cdot x_{i_1} + (x_{i_1} x_{i_2}) \cdot y_j, & i_1 > i_2. \end{cases}$$

Здесь $\cdot$ — знак модульного умножения, $y_{j_2} y_{j_1}$ и $x_{i_1} x_{i_2}$ — лиевы произведения соответствующих элементов алгебр B и A.

Лемма 1. *В принятых обозначениях имеют место следующие утверждения*:

1) *подмодуль* $M_3 = \langle Z_1 \cup Z_2 \rangle$ *модуля* M *изоморфен* $M_1 \oplus M_2$;
2) *фактор-модуль* M/M_3 *изоморфен модулю* M_0.

Доказательство. Для доказательства леммы на векторном пространстве $M' = M_0 \oplus M_1 \oplus M_2$ зададим структуру $R_{X\cup Y}$-модуля таким образом, чтобы векторное пространство $M_1 \oplus M_2$ было подмодулем M' и чтобы индуцированная на нем модульная структура совпадала с исходной. Понятно, что необходимо задать действие кольца $R_{X\cup Y}$ только на аддитивных порождающих M_0 корректным образом. Напомним, что модуль M_0 изоморфен идеалу кольца $R_{X\cup Y}$, порожденному множеством $\{x_i y_j \mid i \in I,\ j \in J\}$; следовательно, аддитивной базой служат всевозможные мономы от букв $X \cup Y$, в записи которых встречается как буква из X, так и буква из Y. Обозначим через W множество всех таких мономов, записанных в лексикографическом порядке по X и по Y.

Если $w \in W$, то запишем w в виде

$$w = (x_i y_j) w^*, \tag{2}$$

где i, j — наименьшие индексы букв X и Y среди встречающихся в записи w.

Пусть V — множество всех мономов от букв $X \cup Y$. Определим модульное действие $w \cdot v$ элемента w из W на моном v из V индукцией по степени монома v, полагая

$$w \cdot x_{i_1} = \begin{cases} (x_i y_j) \cdot w^* x_{i_1}, & \text{если} \quad i_1 \geqslant i, \\ (x_{i_1} y_j) \cdot w^* x_i + (x_i x_{i_1}) \cdot w^* y_j, & \text{если} \quad i_1 < i. \end{cases} \tag{3}$$

Здесь $m = (x_i x_{i_1}) \cdot w^* y_j$ — элемент из M_1, $x_i x_{i_1}$ — лиево произведение в алгебре A,

$$w \cdot y_{j_1} = \begin{cases} (x_i y_j) \cdot w^* y_{j_1}, & \text{если } \ j_1 \geqslant j, \\ (x_i y_{j_1}) \cdot w^* y_j + (y_{j_1} y_j) \cdot w^* x_i, & \text{если } \ j_1 < j, \end{cases} \tag{4}$$

причем $m = (y_{j_1} y_j) \cdot w^* x_i \in M_2$.

Можно проверить, что формулы (3) и (4) можно расширить до задания требуемой модульной структуры на M'.

По построению ясно, что модуль M' порождается теми же элементами (по их написанию), что и модуль M, и что все соотношения (1) модуля M выполнены и на M'. Следовательно, существует гомоморфизм ϕ из M в M'. Покажем, что ϕ является изоморфизмом. Рассмотрим естественную аддитивную базу $\mathscr{B}$ для модуля M'. Прообраз $\mathscr{B}$ порождает M, причем все модульные соотношения на $\mathscr{B}$ выполнены и для ее прообраза. Отсюда $\phi(M_3) = M_1 \oplus M_2$, и гомоморфизм ϕ является изоморфизмом. Лемма 1 доказана. □

Далее, по модулю M построим метабелеву алгебру Ли C. Пусть V — векторное пространство с базой $X \cup Y$ над полем k и пусть $C = V \oplus M$ — прямая сумма векторных пространств над k. Определим на C умножение. Пусть $c_i \in C$, $c_i = (v_i, m_i)$, $i = 1, 2$, $v_i \in V$, $m_i \in M$ — пара элементов из C. Положим

$$(v_1, m_1) \circ (v_2, m_2) = (0, v_1 \cdot v_2 - m_2 \cdot v_1 + m_1 \cdot v_2), \tag{5}$$

где $v_1 v_2$ определяется следующим образом:

$$v_1 v_2 = \begin{cases} x_i x_j & \text{в алгебре } A, \quad \text{если } v_1 = x_i \text{ и } v_2 = x_j, \\ y_i y_j & \text{в алгебре } B, \quad \text{если } v_1 = y_i \text{ и } v_2 = y_j, \\ x_i y_j & \text{элемент } M, \quad \text{если } v_1 = x_i \text{ и } v_2 = y_j, \\ -x_i y_j & \text{элемент } M, \quad \text{если } v_1 = y_i \text{ и } v_2 = x_j, \\ 0, & \text{если } v_1 = 0 \text{ или } v_2 = 0. \end{cases}$$

Если же v_1 и/или v_2 суть линейные комбинации элементов из $X \cup Y$, то умножение v_1 на v_2 определяем по дистрибутивности.

Пусть C — алгебра с введенными выше операциями и пусть $U(C) = \{(0, m) \mid m \in M\}$.

Лемма 2. *Множество $U(C)$ — абелев идеал алгебры C, $C^2 = U(C)$ и C — метабелева алгебра Ли.*

Доказательство. Доказательство леммы непосредственно следует из операций в алгебре C. □

Лемма 3. *В алгебре C выполняются тождество антикоммутативности ($x^2 = 0$) и тождество Якоби. Следовательно, C является метабелевой алгеброй Ли.*

Доказательство. 1. Тождество антикоммутативности непосредственно следует из (5).

2. Докажем выполнение на C тождества Якоби. Пусть $x = (v_1, m_1)$, $y = (v_2, m_2)$, $z = (v_3, m_3)$ — тройка элементов из C. Тогда

$$x \circ y \circ z = (0, (v_1 v_2) v_3 + (m_1 v_2) v_3 - (m_2 v_1) v_3),$$
$$x \circ y \circ z + y \circ z \circ x + z \circ x \circ y = (0, (v_1 v_2) v_3 + (v_2 v_3) v_1 + (v_3 v_1) v_2).$$

Проверим, что имеет место соотношение

$$(v_1 v_2) v_3 + (v_2 v_3) v_1 + (v_3 v_1) v_2 = 0. \tag{6}$$

Равенство (6) достаточно проверить только для случая, когда $v_i \in X \cup Y$, $i = 1, 2, 3$. Если все буквы v_i, $i = 1, 2, 3$, содержатся в X (или Y), то (6) следует из тождества Якоби в алгебре A (соответственно, B). В смешанном случае, в силу симметрии между X и Y, достаточно рассмотреть только случай, когда $v_1 = x_{i_1}$, $v_2 = x_{i_2}$, $v_3 = y_j$. Тогда имеем

$$(v_1 v_2) v_3 + (v_2 v_3) v_1 + (v_3 v_1) v_2 = (x_{i_1} x_{i_2}) \cdot y_j + (x_{i_2} y_j) \cdot x_{i_1} - (x_{i_1} y_j) \cdot x_{i_2}.$$

Рассмотрим три случая.

(i) Если $x_{i_1} = x_{i_2}$, то соотношение (6) верно.
(ii) Если $x_{i_1} > x_{i_2}$, то $(x_{i_1}y_j)\cdot x_{i_2} = (x_{i_1}x_{i_2})\cdot y_j + (x_{i_2}y_j)\cdot x_{i_1}$ и соотношение (6) также верно.
(iii) Случай $x_{i_2} > x_{i_1}$ проверяется аналогично.

Лемма доказана. □

Вернемся к алгебре $A * B$. Ясно, что она допускает систему порождающих $X \cup Y \cup Z_1 \cup Z_2$. В силу категорного определения 2 метабелева произведения существует естественный гомоморфизм $\psi : A * B \to C$.

Теорема 1. *Гомоморфизм ψ является изоморфизмом, причем $\psi(A * B)^2 \simeq U(C) \simeq M$. Коммутант A^2 порождает в $(A * B)^2$ подмодуль, изоморфный M_1, а B^2 — подмодуль, изоморфный M_2. Фактор-модуль $(A * B)^2/M_1 \oplus M_2$ изоморфен M_0.*

Доказательство. Выберем естественный аддитивный базис алгебры C и его естественный прообраз в алгебре $A * B$. Непосредственные вычисления показывают, что полученное множество элементов из $A * B$ является множеством аддитивных порождающих (см. [1]). Отсюда следует, что ψ — изоморфизм, а все остальные утверждения теоремы 1 непосредственно вытекают из этого. □

Теорема 2. *Пусть A и B — абелевы алгебры Ли над k, A — векторное пространство над X, а B — над Y. Тогда $R_{X\cup Y}$-модуль $(A * B)^2$ изоморфен M_0.*

Доказательство. Из условий теоремы получаем, что $A = \overline{A}$ и $B = \overline{B}$, поэтому теорема 2 непосредственно вытекает из теоремы 1, ибо в этом случае $M_1 = M_2 = 0$. □

Предложение 1. *Радикал Фиттинга алгебры $A * B$, $A \neq 0$, $B \neq 0$, совпадает с ее коммутантом*:

$$\mathrm{Fit}(A * B) = (A * B)^2.$$

Доказательство. В метабелевой алгебре Ли радикал Фиттинга не меньше коммутанта. Докажем обратное включение от противного. Возьмем $a \in \mathrm{Fit}(A * B)$, $a \notin (A * B)^2$. Рассмотрим элемент $c = x_i y_j$, где $x_i \in X, y_j \in Y$ — наименьшие элементы из X и Y соответственно. Пусть $a = v_1 + v_2 + m$, где v_1 — линейная комбинация элементов из X, а v_2 — линейная комбинация элементов из Y, $m \in (A*B)^2$. Тогда из определений операций в алгебре $C \simeq A*B$ и предположения, что $a \notin (A*B)^2$, получаем $c \circ \underbrace{a \circ \cdots \circ a}_{n \text{ раз}} \neq 0$. Так как $a, ca \in \langle a\rangle$, то идеал $\langle a\rangle$ не является нильпотентным, а поэтому $a \notin \mathrm{Fit}(A * B)$, противоречие. □

4. Полуобласти

В данном разделе будет введено определение делителей нуля в алгебрах Ли, определения полуобласти и строгой полуобласти, а также будет установлен критерий того, что алгебра $A * B$ является полуобластью.

Пусть A — алгебра Ли над полем k.

Определение 3. Ненулевой элемент $x \in A$ назовем *делителем нуля*, если существует ненулевой элемент $y \in A$ такой, что

$$\langle x\rangle \circ \langle y\rangle = 0. \tag{7}$$

Определение 3 симметрично относительно x и y, поэтому также будем говорить, что x, y — пара делителей нуля.

Если A — метабелева алгебра Ли, то нетрудно проверить, что свойство пары x, y быть парой делителей нуля эквивалентно следующему условию:

$$xy = 0, \quad axy = 0 \quad \forall a \in A. \tag{8}$$

Условие (8) также симметрично относительно x и y. В силу тождества Якоби имеем

$$ayx = xya + axy.$$

Пример 1. Пусть A — нильпотентная алгебра Ли степени нильпотентности n. Тогда любой ее элемент является делителем нуля. Действительно, пусть $x \in A$. Покажем, что существует ненулевой элемент $y \in A$ такой, что $\langle x\rangle \circ \langle y\rangle = 0$. Выберем в качестве y ненулевой элемент из центра алгебры A. Тогда идеал $\langle y\rangle$ есть одномерное векторное пространство, натянутое на y, и условие (7) выполнено.

Пример 2. Пусть A — произвольная алгебра Ли. Тогда любой элемент из $\mathrm{Fit}(A)$ является делителем нуля. Пусть $x \in \mathrm{Fit}(A)$ и $\langle x\rangle$ — главный идеал, порожденный элементом x. Тогда $\langle x\rangle$ — нильпотентный идеал. Проводя рассуждения из примера 1, получаем требуемое.

Пример 3. Пусть A — метабелева алгебра Ли, x, y — такие ее ненулевые элементы, что $xy = 0$ и $x \in A^2$. Тогда x, y — пара делителей нуля. Это следует из того, что для любого элемента $a \in A$ имеем $ay \in A^2$, так что условие (8) выполнено.

Обозначим через $D(A)$ множество делителей нуля алгебры A вместе с нулем.

Определение 4. Алгебра Ли A называется *полуобластью*, если

$$D(A) = \mathrm{Fit}(A).$$

Как показано в примере 2, включение $D(A) \supseteq \mathrm{Fit}(A)$ справедливо для любой алгебры Ли.

В [3] введено понятие *матричной метабелевой алгебры Ли*, которая строится по свободному модулю над кольцом многочленов. Легко проверить, что любая матричная метабелева алгебра Ли является полуобластью.

Пример 4 (не полуобласти)**.** Метабелеву алгебру Ли A зададим следующим образом:

$$A = \langle a_1, a_2, a_3 | a_1a_2a_3 = 0\rangle_{\mathscr{A}^2}.$$

Положим $x = a_1a_2$, $y = a_3$. Тогда $x \in A^2$, $y \notin A^2$ и $xy = 0$, поэтому x и y — пара делителей нуля. Рассмотрим произведение $a_3a_1a_3a_3 \cdots a_3 \neq 0$. Следовательно, идеал $\langle a_3\rangle$ не нильпотентен и $y \notin \mathrm{Fit}(A)$; получаем, что A — не полуобласть.

Определение 5. Алгебра Ли A называется *строгой полуобластью*, если

$$D(A) = A^2.$$

Пусть A — метабелева алгебра Ли; тогда $\mathrm{Fit}(A) \supseteq A^2$. Поэтому верно и включение $D(A) \supseteq A^2$. Отсюда получаем, что A является строгой полуобластью тогда и только тогда, когда A — полуобласть и $\mathrm{Fit}(A) = A^2$.

Из примера 3 следует, что если метабелева алгебра Ли A является строгой полуобластью, то для любых ненулевых элементов $x, y \in A$

$$x \in A^2, \quad y \notin A^2 \quad \Rightarrow \quad xy \neq 0. \tag{9}$$

Другими словами, коммутант A^2 как модуль над кольцом многочленов не имеет кручения при умножении на линейные многочлены. В таких случаях мы будем говорить, что модуль не имеет *линейного кручения*.

Теорема 3 (критерий строгой полуобласти)**.** *Ненулевая метабелева алгебра Ли A является строгой полуобластью тогда и только тогда, когда A неабелева и A^2 как модуль над кольцом многочленов не имеет линейного кручения.*

Доказательство. Предположим, что A является строгой полуобластью. Тогда, как было отмечено выше, для любых ненулевых элементов $x, y \in A$ верно (9). Если A — абелева алгебра Ли, то $A^2 = 0$ и $D(A) = A$. Таким образом, A неабелева. Теперь пусть A неабелева и верно (9). Покажем, что

A — строгая полуобласть. Возьмем произвольную пару x, y ненулевых делителей нуля и покажем, что $x, y \in A^2$.

Допустим сначала, что $x \in A^2$. Тогда из (9) следует, что $y \in A^2$. Теперь предположим, что $x \notin A^2$. Так как A неабелева, то найдется ненулевой элемент $z \in A^2$. Тогда из (9) получаем, что $zx \neq 0$. Поскольку x, y — пара делителей нуля, то $zxy = 0$. Следовательно, zx, y — тоже пара делителей нуля. Отсюда, рассужая так же, как и выше, получаем, что $y \in A^2$, следовательно, $x \in A^2$, противоречие. □

Следствие 1. *Коммутант A^2 ненулевой метабелевой алгебры Ли A не имеет линейного кручения тогда и только тогда, когда алгебра A абелева или является строгой полуобластью.*

Теперь рассмотрим алгебру $A * B$ — метабелево произведение метабелевых алгебр Ли A и B. Структура этой алгебры проанализирована в предыдущем разделе, где установлено, что $\mathrm{Fit}(A * B) = (A * B)^2$. Следовательно, свойства являться полуобластью и строгой полуобластью для алгебры $A * B$ совпадают.

Выше было показано, что строение коммутанта $(A * B)^2$ определяется тремя модулями M_0, M_1 и M_2 над кольцом многочленов $R_{X\cup Y} = k[X \cup Y]$. При этом модуль M_0 не имеет кручения, но для модулей M_1 и M_2 мы не можем утверждать того же (например, потому, что они содержат подмодули A^2 и B^2). Однако справедлива следующая лемма.

Лемма 4. *Пусть коммутант A^2 алгебры A как модуль не имеет линейного кручения. Тогда модуль M_1 также не имеет линейного кручения.*

Доказательство. Возьмем $u \in M_1$ и ненулевой линейный многочлен $f \in R_{X\cup Y}$:

$$f = \sum \alpha_i x_i + \sum \beta_j y_j.$$

Выделим в u слагаемое со старшим одночленом от букв алфавита Y:

$$u = u_1 + a \otimes y_{j_1}^{g_1} \cdots y_{j_t}^{g_t}, \quad 0 \neq a \in A^2.$$

Пусть $\sum \beta_j y_j \neq 0$ и y_{j_n} — наибольший элемент с ненулевым коэффициентом в этой комбинации. Тогда в произведении $u \cdot f$ слагаемое $\beta_j a \otimes y_{j_1}^{g_1} \cdots y_{j_t}^{g_t} \cdot y_{j_n}$ не равно нулю и не сократится.

Если же $\sum \beta_j y_j = 0$, то $\sum \alpha_i x_i \neq 0$. По условию A^2 не имеет линейного кручения: $a \cdot \sum \alpha_i x_i \neq 0$. Поэтому в произведении $u \cdot f$ слагаемое $(a \cdot \sum \alpha_i x_i) \otimes y_{j_1}^{g_1} \cdots y_{j_t}^{g_t}$ не сократится. Таким образом, мы имеем $u \cdot f \neq 0$, что и требовалось показать. □

Теорема 4. *Пусть A и B — ненулевые метабелевы алгебры Ли над полем k, $A * B$ — их метабелево произведение. Тогда алгебра $A * B$ является полуобластью в том и только том случае, когда каждая из алгебр A и B либо абелева, либо является строгой полуобластью.*

Доказательство. Как мы уже упоминали, понятия полуобласти и строгой полуобласти для алгебры $A * B$ равносильны. Поскольку A и B — ненулевые алгебры, то алгебра $A * B$ неабелева. Согласно теореме 3 алгебра $A * B$ является полуобластью тогда и только тогда, когда ее коммутант $(A * B)^2$ не имеет линейного кручения.

Предположим, что алгебра A неабелева и не является строгой полуобластью. Тогда коммутант A^2 имеет линейное кручение, т.е. в A существуют ненулевые элементы $x \in A^2$, $y \notin A^2$ такие, что $xy = 0$. Но тогда $x \in (A * B)^2$, $y \notin (A * B)^2$, т.е. коммутант $(A * B)^2$ имеет линейное кручение. Согласно теореме 3 $A * B$ не является полуобластью.

Теперь предположим, что каждая из алгебр A и B либо абелева, либо является строгой полуобластью. Тогда коммутанты A^2 и B^2 не имеют линейного кручения. Покажем, что в этом случае коммутант $(A * B)^2$ также не имеет линейного кручения.

Возьмем ненулевой элемент $c \in (A * B)^2$ и линейный многочлен $f \in R_{X\cup Y}$:

$$f = \sum \alpha_i x_i + \sum \beta_j y_j.$$

Необходимо показать, что $c \cdot f \neq 0$.

Так как M_0 не имеет кручения, то соотношение $c \notin M_1 \oplus M_2$ означает, что $c \cdot f \neq 0$. Поэтому предположим, что $c \in M_1 \oplus M_2$, и запишем элемент c в виде суммы:

$$c = u + v,\ u \in M_1,\ v \in M_2.$$

Из леммы 4 следует, что хотя бы одно из произведений $u \cdot f$ и $v \cdot f$ не равно нулю. Так как $M_1 \cap M_2 = \emptyset$, то $u \cdot f + v \cdot f \neq 0$, т.е. $c \cdot f \neq 0$, что и требовалось доказать. □

СПИСОК ЛИТЕРАТУРЫ

1. *Артамонов В. А.* Проективные метабелевы алгебры Ли конечного ранга// Изв. Акад. наук СССР. Сер. мат. — 1972. — *36*. — С. 510–522.
2. *Бахтурин Ю. А.* Тождества в алгебрах Ли. — М: Наука, 1985.
3. *Данияров Э. Ю., Казачков И. В., Ремесленников В. Н.* Алгебраическая геометрия над свободной метабелевой алгеброй Ли. I. U-алгебры и универсальные классы// Фундам. прикл. мат. (в печати).
4. *Данияров Э. Ю., Казачков И. В., Ремесленников В. Н.* Алгебраическая геометрия над свободной метабелевой алгеброй Ли. II. Случай конечного поля// Фундам. прикл. мат. (в печати).
5. *Данияров Э. Ю., Казачков И. В., Ремесленников В. Н.* Алгебраическая геометрия над свободной метабелевой алгеброй Ли. I. U-алгебры и A-модули/ Препринт № 34. — Омск: ОмГАУ, 2001.
6. *Baumslag G., Myasnikov A. G., Remeslennikov V. N.* Algebraic geometry over groups. I. Algebraic sets and ideal theory// J. Algebra. — 1999. — *219*. — С. 16–79.
7. *Myasnikov A. G., Remeslennikov V. N.* Algebraic geometry over groups. II// J. Algebra. — 2000. — *234*. — С. 225–276.

Э. Ю. Данияров
Омский филиал Института математики им. С. Л. Соболева Сибирского отделения РАН
E-mail: evelina.omsk@list.ru

И. В. Казачков
Омский филиал Института математики им. С. Л. Соболева Сибирского отделения РАН
E-mail: kazatchkov@iitam.omsk.net.ru

В. Н. Ремесленников
Омский филиал Института математики им. С. Л. Соболева Сибирского отделения РАН
E-mail: remesl@iitam.omsk.net.ru

Современная математика и ее приложения. Том 14 (2004). С. 11–14

УДК 512.552

АНАЛОГ ПРОБЛЕМЫ МАГНУСА ДЛЯ АССОЦИАТИВНЫХ АЛГЕБР

© 2004 г. **В. ДОЦЕНКО, Н. ИЫУДУ, Д. КОРЫТИН**

Аннотация. Доказывается аналог теоремы Магнуса для ассоциативных алгебр без единицы над произвольными полями: если алгебра задается $n+k$ образующими и k соотношениями, а также допускает n-элементную систему образующих, то эта алгебра — свободная алгебра ранга n.

Напомним два теоретико-групповых утверждения, касающихся свободных подгрупп в конечно представимых группах. Теорема Магнуса [5, 6] утверждает, что *если группа G задается с помощью $n+k$ образующих и k соотношений, а также имеет систему из n образующих, то G — свободная группа ранга n*. Следующая теорема доказана И. С. Романовским [1]: *пусть G — группа, заданная $n+k$ образующими и k соотношениями. Тогда в G существует свободная подгруппа ранга n. Кроме того, образующие этой свободной подгруппы можно выбрать из исходных образующих рассматриваемой группы.* Аналоги обеих теорем для полугрупп были доказаны Л. М. Шниерсоном [2]. Вторая теорема (условие Линдона) для ассоциативных алгебр над бесконечным полем была анонсирована в [3] и доказана в [4] для алгебр Ли над произвольным полем. В данной работе приводится доказательство аналога теоремы Магнуса для ассоциативных алгебр без единицы над произвольным полем.

Основная теорема. *Пусть A — ассоциативная алгебра без единицы над полем $\Bbbk$, заданная $n+k$ образующими и k соотношениями. Если A имеет систему образующих $g_1, \dots, g_n$, состоящую из n элементов, то A является свободной алгеброй ранга n.*

Зафиксируем сначала представление A:

$$A = \Bbbk\langle X\rangle / I, \quad I = \mathrm{id}(h_1, \dots, h_k), \quad h_i \in \Bbbk\langle X\rangle,$$

где $X = \{x_1, \dots, x_{n+k}\}$. Считаем, что свободная ассоциативная алгебра $\Bbbk\langle X\rangle$ снабжена обычной функцией степени (предполагается, что все переменные имеют степень 1). Обозначим линейную часть (однородную часть степени 1) элемента $g \in \Bbbk\langle X\rangle$ через Lg. Напомним два простых общих факта.

Предложение 1. *Пусть $V = \{v_1, \dots, v_n\}$, $V \subset \Bbbk\langle X\rangle$, — система элементов степени 1 и пусть система $W = \{w_1, \dots, w_n\}$ получена из V с помощью невырожденного линейного преобразования. Тогда алгебраическая независимость V эквивалентна алгебраической независимости W.*

Следствие 1. *Система $V = \{v_1, \dots, v_n\}$, $V \subset \Bbbk\langle X\rangle$, элементов степени 1 алгебраически независима в том и только том случае, если она линейно независима.*

Пусть $g_1, \dots, g_n$ — система образующих A. Для удобства будем писать g_{n+j} вместо h_j. Обозначим также линейные части многочленов $g_1, \dots, g_{n+k}$ через $y_1, \dots, y_{n+k}$; тогда $Lg_j = y_j$.

Теорема 1. *Система $\{Lg_1, \dots, Lg_{n+k}\}$ алгебраически независима.*

Доказательство. В силу следствия 1 нужно проверить, что y_j линейно независимы. Так как $g_1, \dots, g_n$ порождают фактор

$$A = \Bbbk\langle x_1, \dots, x_{n+k}\rangle / \mathrm{id}(g_{n+1}, \dots, g_{n+k}),$$

получаем, что

$$x_i = \Phi_i(g_1, \dots, g_n) + d_i, \quad d_i \in \mathrm{id}(g_{n+1}, \dots, g_{n+k}) \tag{1}$$

ISSN 1512–1712

для любого $i = 1, \dots, n+k$. Сравнивая линейные части этих соотношений, получаем, что

$$x_i = \sum_{r=1}^{n+k} \alpha_r^i y_r, \quad \alpha_r^i \in \Bbbk, \tag{2}$$

для любого $i = 1, \dots, n+k$. Следовательно, $(n+k)$-элементная система $y_1, \dots, y_{n+k}$ линейно независима. □

Рассмотрим теперь изоморфизм φ свободных алгебр

$$\varphi : \Bbbk\langle x_1, \dots, x_{n+k}\rangle \to \langle y_1, \dots, y_{n+k}\rangle,$$

определенный формулой

$$\varphi(x_i) = \sum_{r=1}^{n+k} \alpha_r^i y_r.$$

Теорема 2. *Система $g_1, \dots, g_n$ алгебраически независима в алгебре*

$$\Bbbk\langle x_1, \dots, x_{n+k}\rangle / \operatorname{id}(g_{n+1}, \dots, g_{n+k})$$

в том и только том случае, если система $\varphi g_1, \dots, \varphi g_n$ алгебраически независима в алгебре

$$\Bbbk\langle y_1, \dots, y_{n+k}\rangle / \operatorname{id}(\varphi g_{n+1}, \dots, \varphi g_{n+k}).$$

Доказательство. Теорема 2 вытекает из того факта, что φ — изоморфизм свободных ассоциативных алгебр. □

Теорема 3. *Система $\varphi g_1, \dots, \varphi g_n$ алгебраически независима в алгебре*

$$A = \Bbbk\langle y_1, \dots, y_{n+k}\rangle / \operatorname{id}(\varphi g_{n+1}, \dots, \varphi g_{n+k}).$$

Доказательство. С помощью описанной выше невырожденной замены переменных получаем следующее свойство:

$$L\varphi g_i = y_i, \quad i = 1, \dots, n+k. \tag{3}$$

В самом деле, поскольку $\varphi(x_i) = \sum \alpha_k^i y_k$, а y_k линейно независимы, то существует обратное преобразование $y_j = \sum \beta_k^j x_k$. Следовательно,

$$L\varphi g_j = \varphi L g_j = \varphi y_j = \sum_k \beta_k^j \varphi x_k = \sum_{k,i} \beta_k^j \alpha_i^k y_i = y_j.$$

Предположим, что существует элемент $\Phi \in \Bbbk\langle z_1, \dots, z_n\rangle$, $\Phi \neq 0$, такой, что

$$\Phi(\varphi g_1, \dots, \varphi g_n) = d, \quad d \in \operatorname{id}(\varphi g_{n+1}, \dots, \varphi g_{n+k}).$$

Свойство (3) позволяет сравнивать минимальные однородные части $\Phi(\varphi g_1, \dots, \varphi g_n)$ и d. Однородная часть минимальной степени многочлена $\Phi(\varphi g_1, \dots, \varphi g_n)$ равна

$$M(y_1, \dots, y_n) = \sum_{(i)} \gamma_{(i)} y_{i_1} \dots y_{i_l},$$

где $M(z_1, \dots, z_n)$ — однородная часть минимальной степени для $\Phi(z_1, \dots, z_n)$, $M(y_1, \dots, y_n) \neq 0$, поскольку $y_1, \dots, y_n$ алгебраически независимы. Следовательно, $\Phi(\varphi g_1, \dots, \varphi g_n)$ содержит только переменные $y_1, \dots, y_n$ и не содержит переменных $y_{n+1}, \dots, y_{n+k}$.

Докажем теперь лемму, которая показывает, что минимальные мономы всех ненулевых элементов из идеала $\operatorname{id}(\varphi g_{n+1}, \dots, \varphi g_{n+k})$ содержат одну из переменных $y_{n+1}, \dots, y_{n+k}$. Это противоречие будет означать, что $\Phi(z_1, \dots, z_n) = 0$ и, следовательно, элементы $\varphi g_1, \dots, \varphi g_n$ алгебраически независимы.

Рассмотрим ассоциативную алгебру $\Bbbk\langle x_1, \dots, x_{n+k}\rangle$ с упорядочиванием элементов $x_1 < \dots < x_{n+k}$. Она индуцирует степенно-лексикографический порядок $\langle X\rangle$: $x_{i_1} \dots x_{i_k} < x_{j_1} \dots x_{j_m}$ в том и только том случае, если $k < m$ или $k = m$ и существует l такой, что $x_{i_l} < x_{j_l}$ и $x_{i_s} = x_{j_s}$ при $s < l$.

Для элемента $s \in \Bbbk\langle X\rangle$ обозначим через $m(s)$ минимальный моном (относительно степенно-лексикографического порядка), появляющийся в многочлене s с ненулевым коэффициентом.

Лемма 1. *Пусть $f_1, \dots, f_k \in \Bbbk\langle x_1, \dots, x_{n+k}\rangle$ и пусть линейная часть f_i есть x_i при любом i: $Lf_i = x_i$. Кроме того, пусть $I = \mathrm{id}(f_1, \dots, f_k)$ — идеал, порожденный $f_1, \dots, f_k$. Тогда для любого элемента $s \in I$ его минимальный моном $m(s)$ содержит по крайней мере одну из переменных $x_1, \dots, x_k$.*

Доказательство. Для любого представления многочлена s с помощью системы элементов $f_1, \dots, f_k$ определим понятие параметра представления.

Определение 1. Пусть $\Pi(s)$ — представление $s \in \Bbbk\langle X\rangle$ с помощью системы $F = \{f_1, \dots, f_k\} \subset \Bbbk\langle X\rangle$:

$$s = \Pi(s) = \sum_{i,\alpha_i} c_{\alpha_i} p_{\alpha_i} f_i q_{\alpha_i},$$

где $c_{\alpha_i} \in \Bbbk \setminus \{0\}$ и $p_{\alpha_i}, q_{\alpha_i} \in \langle X\rangle$. Тогда *параметр τ представления* $\Pi(s)$ — это минимальный моном, появляющийся в этом представлении:

$$\tau = \min_{i,\alpha_i,j} p_{\alpha_i} u_j(f_i) q_{\alpha_i},$$

где $u_j(f_i)$ — мономы многочлена f_i.

Докажем (при наших предположениях), что для любого $s \in \mathrm{id}(f_1, \dots, f_k)$ существует представление с параметром $m(s)$. Для любого элемента $s \in \mathrm{id}(f_1, \dots, f_k)$ имеем некоторое представление

$$s = \sum_{\alpha_i; i=1,\dots,k} c_{\alpha_i} p_{\alpha_i} f_i q_{\alpha_i},$$

где $c_{\alpha_i} \in \Bbbk \setminus \{0\}$, а p_{α_i} и q_{α_i} — мономы. Рассмотрим те элементы этой суммы, для которых $p_{\alpha_i} x_i q_{\alpha_i}$ равен параметру $\tau(\Pi(s))$ этого представления. Ясно, что $\tau \leqslant m(s)$. Если $\tau = m(s)$, то утверждение справедливо. Пусть $\tau < m(s)$ и

$$M = \sum_{i,\alpha_i : p_{\alpha_i} x_i q_{\alpha_i} = \tau} c_{\alpha_i} p_{\alpha_i} f_i q_{\alpha_i}. \tag{4}$$

Так как $\tau < m(s)$, то $M = 0$. Получим новое представление s, если при всех $i = 1, \dots, k$ заменить x_i на $f_i - (f_i - x_i)$ во всех мономах p_{α_i} и q_{α_i} в сумме M в $\Pi(s)$. Так как сумма M равна нулю, то такая же сумма с x_i, замененными на f_i, также равна нулю. Кроме того, если удалить последнюю сумму из нового представления, то опять получится представление s, параметр которого больше, чем τ, поскольку $m(f_i - x_i) > x_i$. Следовательно, получаем новое представление s с большим параметром. Если новый параметр все еще меньше, чем $m(s)$, то можно применить описанную процедуру для получения другого представления с большим параметром и т. д. Так как он не может стать большим, чем $m(s)$, то этот процесс заканчивается, и мы получаем представление s с параметром $m(s)$. Так как параметр любого представления с помощью $f_1, \dots, f_k$ содержит по крайней мере одну из переменных $x_1, \dots, x_k$, то получаем утверждение леммы. □

Как уже отмечалось, доказательство леммы 1 заканчивает и доказательство теоремы 3. □

Теперь основная теорема вытекает из теорем 2 и 3.

Благодарность. Авторы выражают благодарность В. Н. Латышеву, обратившему их внимание на эту комбинаторную задачу.

СПИСОК ЛИТЕРАТУРЫ

1. *Романовский И. С.* Свободные подгруппы в конечно представимых группах// Алгебра и логика. — 1978. — *16*. — С. 62–68.
2. *Шниерсон Л. М.* О свободных подгруппах в конечно представимых группах// Сиб. мат. ж. — 1974. — *15*. — С. 325–328.
3. *Шниерсон Л. М.* О свободных подалгебрах в конечно представисмых алгебрах// Тр. IV Всес. симп. «Теория колец, алгебр и модулей». — Кишинев, 1980. — С. 117–118.
4. *Kharlampovich O. G.* Lyndon's condition for solvable Lie algebras// Sov. Math. — *28*, № 9 (286). — С. 50–59.
5. *Magnus W.* Über freie Faktorgruppen und freie Untergruppen gegebener Gruppen// Monatsh. Math. Phys. — 1939. — *47*. — С. 307–313.
6. *Magnus W., Karrass A., Solitar D.* Combinatorial Group Theory: Presentation of Groups in Terms of Generators and Relations. — N.Y.: Wiley, 1966.

В. Доценко
Московский государственный университет,
Московский независимый университет
Н. Иыуду
Московский государственный университет
E-mail: ioudu@mail.ru

Д. Корытин
Московский государственный университет

Современная математика и ее приложения. Том 14 (2004). С. 15–19

УДК 512.55

ФАКТОРИЗАЦИЯ ЧЕНА—ФОКСА—ЛИНДОНА ДЛЯ СЛОВ НАД ЧАСТИЧНО УПОРЯДОЧЕННЫМ МНОЖЕСТВОМ

© 2004 г. **М. ХАЗЕВИНКЕЛЬ**

Аннотация. Теорема факторизации Чена—Фокса—Линдона для слов над вполне упорядоченным множеством — хорошо известная и важная теорема; ее приложения связаны с итерированными интегралами Чена и используются в теории управления и теории фильтрации. Дается естественное обобщение этой теоремы на случай слов над частично упорядоченными множествами, который возникает в связи с теоремами порождения для (обобщенных) перекрывающих тасовочных алгебр.

СОДЕРЖАНИЕ

1. Введение, определения и формулировка результатов

Пусть A — вполне упорядоченное множество, W — множество слов над A, содержащее пустое слово. Лексикографический порядок на множестве слов над A, т.е. над W, определяется следующим образом. Пусть

$$v = a_1 a_2 \cdots a_m, \quad w = b_1 b_2 \cdots b_n$$

— два слова. Тогда

$$v >_{\mathrm{lex}} w \quad \Longleftrightarrow \quad \begin{cases} \exists i \leqslant \min(m,n) \quad \text{такое, что} \quad a_1 = b_1,\ \ldots,\ a_{i-1} = b_{i-1},\ a_i > b_i \\ \text{или} \quad m > n \quad \text{и} \quad a_1 = b_1,\ \ldots,\ a_n = b_n. \end{cases} \tag{1.1}$$

Собственные хвосты (собственные суффиксы) слова $v = a_1 a_2 \cdots a_m$ — это слова $a_i \cdots a_m$, $i = 2, \ldots, m$. Пустое слово и слово, состоящее из одной буквы, не имеют собственных хвостов. Непустое слово называется словом Линдона, если оно лексикографически меньше, чем всякий его собственный хвост. Например, если A состоит из первых четырех букв стандартного латинского алфавита с обычным порядком, $A = \{a, b, c, d\}$, то слова

$$b,\ ac,\ aababacaabd$$

являются словами Линдона. Теорема факторизации Чена—Фокса—Линдона [3] (см. также [7]) состоит в следующем.

1.2. Теорема. *Любое непустое слово w может быть единственным образом записано в виде*

$$w = v_1 v_2 \cdots v_k, \tag{1.3}$$

где v_i, $i = 1, \ldots, k$, — слова Линдона и

$$v_1 \geqslant_{\mathrm{lex}} v_2 \geqslant_{\mathrm{lex}} \cdots \geqslant_{\mathrm{lex}} v_k.$$

ISSN 1512–1712

Например,

$$bdcaaddbcacaababacaaa = (bdc)(aaddbcac)(aababac)(a)(a)(a).$$

Эта теорема весьма важна в ряде областей, например, в теории свободных алгебр Ли [8] и теории квазисимметрических функций [6]. Хорошим алгоритмом для нахождения факторизаций Чена—Фокса—Линдона служит алгоритм блочного разложения, описанный в [9] (см. также [5] по поводу доказательства того, что блочное разложение из [9] есть то же самое, что и факторизация Чена—Фокса—Линдона). Существуют другие алгоритмы с линейным временем (см. [7]). Пусть теперь алфавит A всего лишь частично упорядочен. Возникает вопрос о существовании естественного обобщения такой факторизации на этот случай. Конечно, частичный порядок можно продолжить до вполне упорядоченности, однако эта процедура неканоническая.

Определение лексикографического порядка на множестве слов над частично упорядоченным множеством то же, что и в случае вполне упорядоченного множества, т.е. (1.1). Конечно, из него следует, что a_i и b_i сравнимы. Это дает частичный порядок на множестве слов (см. лемму 2.1). Определение слова Линдона также сохраняется. Из него следует, что некоторые пары слов в слове Линдона сравнимы; например, первая буква должна быть сравнима со всеми остальными. Тем не менее не верно утверждение о том, что если слово является словом Линдона, то все его составляющие необходимо сравнимы. Например, если $\{a, b, c, d\}$ имеет частичный порядок, являющийся транзитивным замыканием неравенств $a < b, c$ и $b, c < d$ (где b и c не сравнимы), то $aabacd$ — слово Линдона.

Подходящим обобщением факторизационной теоремы 1.2 является следующее утверждение.

1.4. Теорема (ЧФЛ-факторизация над частично упорядоченными множествами)**.** *Любое непустое слово над частично упорядоченным алфавитом A единственным образом факторизуется в виде*

$$w = t_1 t_2 \cdots t_k, \tag{1.5}$$

где все t_i — слова Линдона и для любого $i = 1, \ldots, k-1$ либо t_i и t_{i+1} несравнимы, либо $t_i \geqslant_{\mathrm{lex}} t_{i+1}$ (т.е. $\neg(t_i < t_{i+1})$).

Заметим, что если A вполне упорядочено, то из этой теоремы вытекает факторизационную теоерему 1.2. В другом крайнем случае, когда частичный порядок тривиален, т.е. все пары различных элементов несравнимы, ЧФЛ-факторизация частичного порядка есть факторизация в слова, состоящие из одной буквы (которые в данном случае являются единственными словами Линдона).

2. Доказательства

Для доказательства факторизационной теоремы Чена—Фокса—Линдона для частично упорядоченных множеств нужны некоторые подготовительные леммы, Некоторые из них аналогичны таковым в обычном случае вполне упорядоченного множества, а некоторые существенно отличаются. Первый шаг состоит в доказательстве того, что лексикографический порядок транзитивен и в случае частично упорядоченного алфавита.

2.1. Лемма. *Пусть A — частично упорядоченный алфавит. Тогда лексикографический порядок на словах, определенный правилом* (1.1)*, транзитивен.*

Доказательство. Введем дополнительную букву θ, меньшую, чем все остальные буквы, и рассмотрим слова над $A \cup \{\theta\}$, индексированные с помощью множества $\mathbb{N} = (1, 2, 3, \ldots)$. Вложим слово над A в множество бесконечных слов над $A \cup \{\theta\}$ путем сопоставления слову $v = a_1 \cdots a_m$ бесконечного слова $v_e = a_1 \cdots a_m \theta\theta\theta \cdots$ и заметим, что

$$w >_{\mathrm{lex}} v \quad \Longleftrightarrow \quad w_e \geqslant_{\mathrm{lex}} v_e.$$

Кроме того, для расширенных слов можно применить только первый случай из (1.1). Это уменьшает число случаев, подлежащих рассмотрению. Пусть

$$v = a_1 a_2 \cdots, \quad w = b_1 b_2 \cdots, \quad u = c_1 c_2 \cdots$$

— бесконечные слова и пусть $v >_{\text{lex}} w$ и $w >_{\text{lex}} u$. Тогда существует индекс i такой, что

$$a_1 = b_1, \quad \dots, \quad a_{i-1} = b_{i-1}, \quad a_i > b_i,$$

и существует индекс j такой, что

$$b_1 = c_1, \quad \dots, \quad b_{j-1} = c_{j-1}, \quad b_j > c_j.$$

Если $j < i$, то

$$a_1 = b_1 = c_1, \quad \dots, \quad a_{j-1} = b_{j-1} = c_{j-1}, \quad a_j \geqslant b_j > c_j,$$

а потому $w >_{\text{lex}} u$. Если $j > i$, то

$$a_1 = b_1 = c_1, \quad \dots, \quad a_{i-1} = b_{i-1} = c_{i-1}, \quad a_i > b_i = c_i,$$

значит, и $w >_{\text{lex}} u$. □

2.2. Лемма. *Пусть $v_1 <_{\text{lex}} v_2$, где v_1 и v_2 — слова Линдона. Тогда $v_1 v_2 <_{\text{lex}} v_2$.*

Доказательство. Пусть $v_1 = a_1 \cdots a_l$ и $v_2 = b_1 \cdots b_k$. Тогда существуют две возможности: $k \leqslant l$ либо $k > l$.

Пусть $k \leqslant l$. Тогда существует число $r \leqslant k$ такое, что

$$b_i = a_i, \quad i = 1, \dots, r-1, \qquad b_r > a_r.$$

Теперь

$$v_1 v_2 = a_1 \cdots a_{r-1} a_r \cdots, \quad v_2 = b_1 \cdots b_{r-1} b_r \cdots,$$

и получаем, что $v_1 v_2 <_{\text{lex}} v_2$.

Пусть $k > l$. Если существует число $r \leqslant l$ такое, что

$$b_i = a_i, \quad i = 1, \dots, r-1, \qquad b_r > a_r,$$

то имеет место ситуация, аналогичная рассмотренной выше. В противном случае

$$a_i = b_i, \quad i - 1, \dots, l,$$

т.е. v_1 — префикс v_2. Тогда

$$v_1 v_2 = a_1 \cdots a_l b_1 \cdots b_k, \quad v_2 = a_1 \cdots a_l b_{l+1} \cdots b_k.$$

Теперь $b_{l+1} \cdots b_k$ — собственный хвост v_2, а v_2 — слово Линдона; значит, $b_{l+1} \cdots b_k$ больше, чем v_2 и, следовательно, $v_1 v_2 <_{\text{lex}} v_2$. □

2.3. Лемма. *Пусть v_1 и v_2 — слова Линдона и $v_1 <_{\text{lex}} v_2$. Тогда $v_1 v_2$ — слово Линдона.*

Доказательство. Пусть t — собственный хвост слова $v_1 v_2$. Возможны следующие три случая.

(i) t — собственный хвост v_2. Тогда $t >_{\text{lex}} v_2$ и $v_2 >_{\text{lex}} v_1 v_2$ согласно лемме 2.2. Поэтому $t >_{\text{lex}} v_1 v_2$ (см. лемму 2.1).

(ii) $t = v_2$. Тогда $t = v_2 >_{\text{lex}} v_1 v_2$ согласно лемме 2.2.

(iii) t имеет вид $t = t' v_2$, где t' — собственный хвост v_1. Тогда $t' >_{\text{lex}} v_1$, поскольку v_1 — слово Линдона, а потому $t' v_2 >_{\text{lex}} v_1 v_2$.

Лемма доказана. □

2.4. Лемма. *Если слова $v_1 v_2$ и $v_3 v_4$ сравнимы, то v_1 и v_3 также сравнимы.*

Доказательство. Слова $v_1 = a_1 \cdots a_k$ и $v_3 = b_1 \cdots b_l$ не сравнимы в том и только том случае, если существует число $r \leqslant \min\{k, l\}$ такое, что

$$a_i = b_i, \quad i = 1, \dots, r-1,$$

а a_r и b_r не сравнимы. Это противоречит тому, что слова $v_1 v_2$ и $v_3 v_4$ сравнимы. □

Доказательство теоремы 1.4. *Существование*. Пусть t — хвост слова Линдона w, имеющий максимальную длину. Если $t = w$, то утверждение доказано. Если $t \neq w$, то запишем $w = w't$. По индукции (например, по длине w), имеем

$$w' = t_1 \cdots t_{k-1},$$

где все сомножители — слова Линдона, а $t_i \geqslant_{\text{lex}} t_{i+1}$, если t_i и t_{i+1} сравнимы, $i = 1, \ldots, k-2$. Тогда

$$w = w't = t_1 \cdots t_{k-1}t,$$

где все сомножители — слова Линдона. Предположим, что $t_{k-1} <_{\text{lex}} t$ (если два сомножителя сравнимы, то доказывать нечего). Тогда согласно лемме 2.3 получаем, что $t_{k-1}t$ — слово Линдона; это противоречит максимальности t.

Единственность. Это наиболее трудная часть доказательства, поскольку сомножители в факторизации на сомножители Линдона не обязаны быть сравнимыми.

Пусть

$$w = t_1 \cdots t_k = t'_1 \cdots t'_k$$

— две факторизации. Если $\text{length}(t_k) = \text{length}(t'_l)$, то $t_k = t'_l$. Удалим эти сомножители; по индукции доказательство закончено. В противном случае предположим, что $\text{length}(t_k) > \text{length}(t'_l)$. Поэтому

$$t_k = tt'_l.$$

Предположим, что t — хвост t'_{l-1} или что $t = t'_{l-1}$. Тогда $t \geqslant_{\text{lex}} t'_{l-1}$, поскольку t'_{l-1} — слово Линдона. Более того, $t_k = tt'_l$ — слово Линдона; поэтому

$$t'_l <_{\text{lex}} tt'_l \geqslant_{\text{lex}} t'_{l-1}t'_l. \tag{2.5}$$

Согласно лемме 2.4 это означает, что t'_{l-1} и t'_l сравнимы и, следовательно, $t'_{l-1} \geqslant_{\text{lex}} t'_l$ согласно свойству ЧФЛ-факторизации (см. формулировку теоремы). Поэтому $t'_{l-1}t'_l \geqslant_{\text{lex}} t'_lt'_l$, что вместе с (2.5) и транзитивностью (лемма 2.1) влечет неравенство $t'_l >_{\text{lex}} t'_lt'_l$, чего не может быть.

Это был простейший случай. Рассмотрим теперь случай, когда

$$t_k = tt'_i \cdots t'_l, \tag{2.6}$$

где t — непустой хвост t'_{i-1}. Теперь t_k — слово Линдона и t'_l — его собственный хвост, поэтому

$$t'_l >_{\text{lex}} t_k. \tag{2.7}$$

Далее, t — непустой хвост t'_{i-1}, следовательно,

$$t \geqslant_{\text{lex}} t'_{i-1}. \tag{2.8}$$

Сопоставляя (2.7) и (2.8), находим, что

$$t'_l >_{\text{lex}} t_k = tt'_i \cdots t'_l \geqslant_{\text{lex}} t'_{i-1}t'_i \cdots t'_l. \tag{2.9}$$

Снова используя тот факт, что t_k — слово Линдона, имеем

$$t'_i \cdots t'_l >_{\text{lex}} t_k. \tag{2.10}$$

Сопоставляя это с (2.8), находим, что

$$t'_i \cdots t'_l >_{\text{lex}} t_k = tt'_i \cdots t'_l \geqslant_{\text{lex}} t'_{i-1}t'_i \cdots t'_l. \tag{2.11}$$

Согласно лемме 2.4 отсюда следует, что t'_{i-1} и t'_i сравнимы; следовательно,

$$t'_{i-1} \geqslant_{\text{lex}} t'_i \tag{2.12}$$

в силу факторизационного свойства Чена—Фокса—Линдона. Это дает

$$t'_{i-1}t'_i \cdots t'_l \geqslant_{\text{lex}} t'_it'_i \cdots t'_l. \tag{2.13}$$

Сопоставляя это с (2.11), получаем

$$t'_i \cdots t'_l >_{\text{lex}} t'_it'_i \cdots t'_l; \tag{2.14}$$

отсюда следует, что

$$t'_{i+1}\cdots t'_l >_{\mathrm{lex}} t'_i\cdots t'_l. \tag{2.15}$$

Таким образом, t'_i и t'_{i+1} сравнимы; значит, согласно факторизационному свойству Чена—Фокса—Линдона имеем

$$t'_i \geqslant_{\mathrm{lex}} t'_{i+1}. \tag{2.16}$$

Отсюда

$$t'_i t'_{i+1}\cdots t'_l \geqslant_{\mathrm{lex}} t'_{i+1}t'_{i+1}\cdots t'_l, \tag{2.17}$$

что вместе с (2.15) дает

$$t'_{i+1}\cdots t'_l \geqslant_{\mathrm{lex}} t'_{i+1}t'_{i+1}\cdots t'_l \tag{2.18}$$

и

$$t'_{i+2}\cdots t'_l \geqslant_{\mathrm{lex}} t'_{i+1}\cdots t'_l. \tag{2.19}$$

Согласно лемме 2.4 это делает t'_{i+1} и t'_{i+2} сравнимыми. Действуя (по индукции) таким образом, видим, что все пары t'_r, t'_{r+1}, $r = i-1,\ldots,l-1$, сравнимы и, следовательно,

$$t'_{i-1} \geqslant_{\mathrm{lex}} t'_i \geqslant_{\mathrm{lex}} \cdots \geqslant_{\mathrm{lex}} t'_l. \tag{2.20}$$

Подставляя это в (2.9), получаем

$$t'_l >_{\mathrm{lex}} t'_l t'_i\cdots t'_l, \tag{2.21}$$

что невозможно. Следовательно, предположение о неравенстве длин не выполняется, и доказательство завершено. □

СПИСОК ЛИТЕРАТУРЫ

1. *Хазевинкель М.* Обобщенные перекрывающие тасовочные алгебры// Итоги науки и техн. Совр. мат. и ее прилож. Тематич. обзоры. — М.: ВИНИТИ, 2000. — *69*. — С. 193–222.
2. *Chen K.-T.* Algebras of iterated path integrals and fundamental groups// Trans. Amer. Math. Soc. — 1971. — *156*. — С. 359–379.
3. *Chen K.-T., Fox R. H., Lyndon R. C.* Free differential calculus. IV// *Ann. Math.* — 1958. — *68*. — С. 81–95.
4. *Fliess M.* Intégrales itérées de K. T. Chen, bruit blanc Gaussien etfiltrage nonlinéaire// C. R. Acad. Sci. Paris, Sér. A. — 1977. — *284*. — С. 459–462.
5. *Hazewinkel M.* The Leibniz–Hopf algebra and Lyndon words/ Preprint. — Amsterdam: CWI, 1996.
6. *Hazewinkel M.* The algebra of quasi-symmetric functions is free over the integers// Adv. Math. — 2001. — *164*. — С. 283–300.
7. *Lothaire M.*, ed. Combinatorics on Words. — Addison-Wesley, 1983.
8. *Reutenauer C.* Free Lie Algebras. — Oxford Univ. Press, 1993.
9. *Scholtens A. C. J.* S-Typical curves in noncommutative Hopf algebras/ Ph.D. thesis. — Free Univ. of Amsterdam, 1996.

М. Хазевинкель
CWI, Amsterdam
E-mail: mich@cwi.nl

Современная математика и ее приложения. Том 14 (2004). С. 20–39

УДК 512.55

КОЛЧАНЫ АССОЦИАТИВНЫХ КОЛЕЦ

© 2004 г. **В. В. КИРИЧЕНКО**

Аннотация. Понятие колчана, т.е. ориентированного графа конечномерной алгебры было введено П. Габриэлем в связи с задачами теории представлений конечномерных алгебр. Понятие схемы-колчана $Q(A)$ полусовершенного нетерова справа кольца A было введено автором и применено для изучения структуры полуцепных колец. Дается краткий обзор некоторых результатов по структурной теории колец, полученных с использованием теории графов.

СОДЕРЖАНИЕ

1. Колчаны нетеровых справа полусовершенных колец

Все кольца предполагаются ассоциативными с $1 \neq 0$. $R = R(A)$ — радикал Джекобсона кольца A. Термины «артиново», «нетерово» и т. д. используются для обозначения двусторонних свойств кольца, например, «артиново кольцо» означает артиново справа и слева кольцо.

Будем говорить, что кольцо A *неразложимо*, если A не может быть представлено в виде прямого произведения двух колец.

Идемпотент $e \in A$ называется *локальным*, если eAe — локальное кольцо.

Теорема 1.1 (см. [32]). *Кольцо A полусовершенно тогда и только тогда, когда единица кольца A может быть представлена в виде суммы попарно ортогональных локальных идемпотентов.*

Обозначим через M^n прямую сумму n экземпляров M и $M^0 = 0$.

Пусть A — полусовершенное нетерово справа кольцо, R — его радикал Джекобсона, $P_1, \ldots, P_s$ $(Q_1, \ldots, Q_s)$ — все попарно неизоморфные правые (левые) проективные неразложимые модули, $U_i = P_i/P_iR$, $V_i = Q_i/RQ_i$ для $i = 1, \ldots, s$, и

$$\bar{A} = A/R = M_{n_1}(\mathscr{D}_1) \times \cdots \times M_{n_s}(\mathscr{D}_s),$$

где $\mathscr{D}_1, \ldots, \mathscr{D}_s$ — тела. Через $M_n(B)$ обозначим кольцо всех $(n \times n)$-матриц над кольцом B.

Работа выполнена при поддержке гранта FAPESP of Brazil Proc. 02/05087-2.

ISSN 1512–1712

Определение 1.2. Пусть $P(P_iR)$ — проективное накрытие P_iR:

$$P(P_iR) = \bigoplus_{j=1}^{s} P_j^{t_{ij}}, \quad i,j = 1,\dots,s.$$

Поставим в соответствие модулям $P_1,\dots,P_s$ вершины $1,\dots,s$ и соединим вершину i с вершиной j t_{ij} стрелками. Полученный конечный ориентированный граф называется *колчаном кольца* A и обозначается $Q(A)$.

Аналогично может быть определен левый колчан $Q'(A)$ нетерова слева полусовершенного кольца A.

Из определения проективного накрытия следует, что $Q(A) = Q(A/R^2)$.

Если A — такое полусовершенное кольцо, что A/R^2 является артиновым справа, то определим $Q(A)$ формулой $Q(A) = Q(A/R^2)$. Если A/R^2 артиново слева, то $Q'(A) = Q'(A/R^2)$.

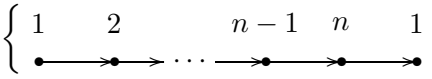
Отметим, что колчаны полусовершенных колец, эквивалентных в смысле Мориты, равны между собой.

Примеры. 1. Колчан полупростого артинова кольца является несвязным объединением точек и имеет вид

$$\{\bullet \qquad \bullet \qquad \cdots \qquad \bullet\}.$$

2. Рассмотрим колчан кольца p-целых чисел $A = \mathbb{Z}_p$, где p — простое число. Это локальное кольцо с единственным неразложимым проективным модулем. Проективное накрытие радикала $R = p\mathbb{Z}_p$ — это A. Поэтому колчан кольца $\mathbb{Z}_p$ является петлей и имеет вид

3. Пусть $A = T_n(D)$ — кольцо верхних треугольных матриц степени n над дискретно нормированным кольцом D. Оно имеет n главных A-модулей вида $P_i = e_{ii}A$, где e_{ii} — матричные единицы. Легко проверить, что $P_iR \simeq P_{i+1}$ для $i = 1,2,\dots,n-1$ и $P_nR = 0$. Следовательно, колчан кольца A — это цепь вида



4. Пусть

$$A = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix},$$

где $\mathbb{Z}_p$ — кольцо p-целых чисел, $\mathbb{Q}$ — поле рациональных чисел. Легко проверить, что колчан $Q(A)$ имеет вид

Кольцо A является кольцом Херстейна—Смолла.

Неразложимая как кольцо алгебра называется обычно *связной*.

Теорема 1.3 (см. [4,5])**.** *Для полусовершенного нетерова кольца A следующие условия эквивалентны*:

1) *A — неразложимое кольцо*;
2) *A/R^2 — неразложимое кольцо*;
3) *колчан $Q(A)$ связен.*

Замечание. Теорема 1.3 неверна для полусовершенных односторонне нетеровых колец. В качестве примера можно рассмотреть кольцо

$$A = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}.$$

Его колчан $Q(A)$ — это несвязное объединение одной петли и одной точки. Очевидно,

$$R^2 = \begin{pmatrix} p^2\mathbb{Z}_p & \mathbb{Q} \\ 0 & 0 \end{pmatrix}.$$

Таким образом, кольцо A/R^2 разлагается в прямое произведение колец

$$A/R^2 \simeq \mathbb{Z}_p/p^2\mathbb{Z}_p \times \mathbb{Q}.$$

Однако кольцо A не разлагается в прямое произведение колец.

Можно доказать, что если колчан полусовершенного нетерова справа неразложимого кольца несвязен, то пересечение натуральных степеней радикала этого кольца не равно нулю.

Предложение 1.4. *Пусть A — полусовершенное кольцо такое, что A/R^2 артиново. Справедливы следующие утверждения.*

1) *Если в $Q(A)$ имеется стрелка из i в j, то в левом колчане $Q'(A)$ имеется стрелка из j в i.*
2) *Если $Q(A)$ имеется стрелка σ_{ij} из i в j, то существует ненулевой гомоморфизм из P_j в P_i и из Q_i в Q_j.*

Доказательство немедленно вытекает из определения колчана $Q(A)$.

Обозначим через Q_u колчан, полученный из Q заменой всех стрелок из i в j одной стрелкой (допускается случай $i = j$). Если в Q нет стрелок из i в j, то их нет и в Q_u.

Обозначим через $\bar{Q}$ неориентированный граф, полученный из Q снятием ориентации.

Следствие 1.5. *Пусть A — полусовершенное кольцо такое, что A/R^2 артиново. Тогда*

$$\overline{Q_u(A)} = \overline{Q'_u(A)}.$$

Доказательство вытекает из предложения 1.4.

Следующую теорему можно рассматривать как один из вариантов теоремы Веддербарна—Артина.

Теорема 1.6 (см. [26, с. 238])**.** *Для полусовершенного нетерова справа кольца A следующие условия равносильны*:

1) *кольцо A полупростое артиново*;
2) *колчан $Q(A)$ является конечным множеством точек.*

Замечание. Автору не известно, верна ли эта теорема для любых полусовершенных колец.

Следующие две леммы являются главным инструментом в теории обычных колчанов полусовершенных колец.

Лемма 1.7 (аннуляторная лемма [5, 26])**.** *Пусть $1 = f_1 + \cdots + f_s$ — каноническое разложение $1 \in A$. Для любого простого правого A-модуля U_i и для каждого f_j имеем*

$$U_i f_j = \delta_{ij} U_i, \quad i, j = 1, \ldots, s.$$

Аналогично, для любого простого левого A-модуля V_i и для каждого f_j имеем

$$f_j V_i = \delta_{ij} V_i, \quad i, j = 1, \ldots, s.$$

Пусть A — приведенное полусовершенное кольцо, т.е. $\bar{A} = A/R$ является конечным прямым произведением тел, $1 = e_1 + \ldots + e_s$ — разложение $1 \in A$ в сумму попарно ортогональных локальных идемпотентов.

Лемма 1.8 (Q-лемма [5, 26]). *Простой модуль U_k (соответственно, V_k) содержится в прямом разложении модуля e_iR/e_iR^2 (соответственно, Re_i/R^2e_i) тогда и только тогда, когда $e_iR^2e_k$ (соответственно, $e_kR^2e_i$) строго содержится в e_iRe_k (соответственно, в e_kRe_i).*

2. Первичный колчан FDD-кольца

Определение 2.1. Кольцо A называется *конечно разложимым* (FD-*кольцом*), если оно разлагается в прямое произведение конечного числа неразложимых колец.

Очевидно, нетеровы справа и полусовершенные кольца являются FD-кольцами.

Теорема 2.2 (см. [26]). *Любое FD-кольцо A может быть единственным образом представлено в виде прямого произведения конечного числа неразложимых колец, т.е. если*

$$A = B_1 \times B_2 \times \ldots \times B_s = C_1 \times C_2 \times \ldots \times C_t$$

— два таких разложения, то $s = t$ и существует подстановка σ чисел $\{1, 2, \ldots, t\}$ такая, что $B_i = C_{\sigma(i)}$ для $i = 1, 2, \ldots, t$.

Обозначим через $\Pr(A)$ первичный радикал кольца A.

Определение 2.3. Факторкольцо $A/\Pr(A)$ называется *диагональю кольца A*.

Диагональ кольца является полупервичным кольцом.

Определение 2.4. Кольцо A называется *кольцом с конечно разложимой диагональю* (сокращенно FDD-*кольцом*), если его диагональ $A/\Pr(A)$ является FD-кольцом.

Можно построить двустороннее пирсовское разложение первичного радикала $\Pr(A)$ произвольного FDD-кольца A следующим образом.

Пусть $\bar{A} = \bar{A}_1 \times \ldots \times \bar{A}_t$ — разложение диагонали $\bar{A} = A/\Pr(A)$ в прямое произведение конечного числа неразложимых колец и $\bar{1} = \bar{f}_1 + \cdots + \bar{f}_t$ — соответствующее разложение единицы $\bar{1} \in \bar{A}$ в сумму попарно ортогональных центральных идемпотентов. Хорошо известно, что $\Pr(A)$ является ниль-идеалом; тогда идемпотенты $\bar{f}_1, \ldots, \bar{f}_t$ можно поднимать по модулю $\Pr(A)$, сохраняя их ортогональность, т.е. имеем равенство

$$1 = f_1 + f_2 + \cdots + f_t,$$

где $f_if_j = \delta_{ij}f_i$ и $\bar{f}_i = f_i + \Pr(A)$ для $i, j = 1, \ldots, t$. Очевидно, $A_{ij} = f_iAf_j \subset \Pr(A)$ ($i \neq j$, $i, j = 1, \ldots, t$) и $\mathscr{I}_i = f_i \Pr(A) f_i$ — первичный радикал $\Pr(A_i)$ кольца $A_i = f_iAf_i$ ($i = 1, \ldots, t$). Двустороннее пирсовское разложение первичного радикала $\Pr(A)$ кольца A имеет вид

$$\Pr(A) = \begin{pmatrix} \mathscr{I}_1 & A_{12} & \ldots & A_{1t} \\ A_{21} & \mathscr{I}_2 & \ldots & A_{2t} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ A_{t1} & A_{t2} & \ldots & \mathscr{I}_t \end{pmatrix}.$$

Более того, $\bar{A} = A/\Pr(A) = A_1/\mathscr{I}_1 \times \ldots \times A_t/\mathscr{I}_t$, т.е. $\bar{A}_k = A_k/\mathscr{I}_k$ для $k = 1, \ldots, t$.

Предложение 2.5 (см. [26, с. 221]). *Первичный радикал FDD-кольца имеет двустороннее пирсовское разложение*

$$\Pr(A) = \bigoplus_{i,j=1}^{t} f_i \Pr(A) f_j,$$

где

$$f_i \Pr(A) f_i = \Pr(A_i) = \mathscr{I}_i, \quad f_i \Pr(A) f_j = A_{ij}, \quad i \neq j,\ i, j = 1, \ldots, t,$$

и, более того,

$$\bar{A} = A/\Pr(A) = A_1/\mathscr{I}_1 \times \ldots \times A_t/\mathscr{I}_t,$$

т.е. $\bar{A}_k = A_k/\mathscr{I}_k$ при $k = 1, \ldots, t$.

Используя наши обозначения, дадим определение первичного колчана для произвольного FDD-кольца.

Определение 2.6. Пусть A — FDD-кольцо с первичным радикалом $\mathscr{I} = \mathrm{Pr}(A)$ и $W = \mathscr{I}/\mathscr{I}^2$. Установим соответствие между идемпотентами $\bar{f}_1, \ldots, \bar{f}_t$ и точками $1, \ldots, t$, связывая вершину i с вершиной j стрелкой с началом в i и концом j тогда и только тогда, когда $\bar{f}_i W \bar{f}_j \neq 0$. Конечный ориентированный граф, полученный таким образом, называется *первичным колчаном FDD-кольца A* и обозначается $PQ(A)$.

Очевидно, $PQ(A) = PQ(A/\mathrm{Pr}^2(A))$ и $PQ(A)$ определяется единственным образом с точностью до нумерации вершин.

Приведем определение T-нильпотентного идеала (правого, левого, двустороннего), которое было введено Х. Бассом (см. [16, с. 466]).

Определение 2.7. Идеал (правый, левый, двусторонний) $\mathscr{J}$ называется *правым* (соответственно, *левым*) *T-нильпотентным*, если для любой последовательности $a_1, a_2, \ldots, a_n \ldots$ элементов $a_i \in \mathscr{J}$ существует целое положительное число k такое, что $a_k a_{k-1} \ldots a_1 = 0$ (соответственно, $a_1 a_2 \ldots a_k = 0$). Идеал $\mathscr{J}$ называется *T-нильпотентным*, если он правый и левый T-нильпотентный.

Ясно, что любой T-нильпотентный идеал является нильидеалом. Однако не каждый T-нильпотентный идеал является нильпотентным. Итак, T-нильпотентные идеалы находятся между нильпотентными и нильидеалами. Следующую теорему можно рассматривать как некоторое обобщение леммы Накаямы для любых правых модулей.

Теорема 2.8 (см. [28, Theorem 11.5.5])**.** *Для правого идеала $\mathscr{I}$ кольца A следующие условия равносильны*:

1) *$\mathscr{I}$ является T-нильпотентным справа правым идеалом*;
2) *правый A-модуль M, удовлетворяющий равенству $M\mathscr{I} = M$, равен нулю*;
3) *для любого ненулевого правого A-модуля M выполняется соотношение $M\mathscr{I} \neq M$*;
4) *$A^I\mathscr{I} \neq A^I$, где A^I — свободный модуль счетного ранга.*

Теорема 2.9 (см. [26, с. 223])**.** *Для кольца A с T-нильпотентным первичным радикалом* $\mathrm{Pr}(A)$ *следующие условия равносильны*:

1) *A неразложимо*;
2) *факторкольцо $A/\mathrm{Pr}^2(A)$ неразложимо.*

Теорема 2.10 (см. [26, с. 224])**.** *Пусть A — FDD-кольцо. Первичный колчан FDD-кольца A с T-нильпотентным первичным радикалом* $\mathrm{Pr}(A)$ *является связным тогда и только тогда, когда кольцо A неразложимо.*

Определение 2.11 (см. [29])**.** Кольцо A с конечной разложимой диагональю будем называть *связным*, если первичный колчан $PQ(A)$ FDD-кольца A связен.

Принимая во внимание факт, что первичный радикал нетерова справа кольца нильпотентен, получаем следующий результат.

Следствие 2.12 (см. [29])**.** *Нетерово справа кольцо единственным образом разлагается в конечное прямое произведение связных колец.*

3. Идеал, ассоциированный с первичным колчаном ассоциативного кольца

Пусть J — двустронний идеал кольца A, содержащийся в радикале Джекобсона R кольца A и такой, что идемпотенты можно поднимать по модулю J.

Определение 3.1. Факторкольцо A/J называется *J-диагональю* кольца A.

Определение 3.2. Кольцо A называется кольцом с конечно разложимой J-диагональю (коротко $FD(J)$-кольцо), если его J-диагональ A/J является FD-кольцом.

Для произвольного $FD(J)$-кольца A построим колчан $Q(A,J)$. Рассмотрим J-диагональ $FD(J)$-кольца A: $\bar{A} = A/J = \bar{A}_1 \times \ldots \times \bar{A}_t$, где все кольца $\bar{A}_1, \ldots, \bar{A}_t$ неразложимые и $\bar{1} = \bar{f}_1 + \ldots + \bar{f}_t$ — соответствующее разложение $\bar{1} \in \bar{A}$ в сумму взаимно ортогональных центральных идемпотентов, т.е. $\bar{f}_i \bar{A} \bar{f}_i = \bar{f}_i \bar{A} = \bar{A} \bar{f}_i = \bar{A}_i$ для $i = 1, \ldots, t$. Положим $W = J/J^2$. Установим соответствие между идемпотентами $\bar{f}_1, \ldots, \bar{f}_t$ и вершинами $1, \ldots, t$, соединяя вершину i с вершиной j стрелкой с началом в i и концом в j тогда и только тогда, когда $\bar{f}_i W \bar{f}_j \neq 0$. Полученный конечный ориентированный граф $Q(A,J)$ будем называть колчаном, ассоциированным с идеалом J.

Принимая во внимание теорему 2.2, легко видеть, что колчан $Q(A,J)$ $FD(J)$-кольца A определен единственным образом с точностью до нумерации вершин и $Q(A,J) = Q(A/J^2, W)$.

По определению колчан $Q(A,J)$ является простым колчаном, а матрица смежности $[Q(A,J)]$ — $(0,1)$-матрицей.

Предположим, что J — двусторонний идеал кольца A, содержащийся в радикале Джекобсона R $FD(J)$-кольца A такой, что идемпотенты можно поднимать по модулю J. Пусть $\bar{A} = A/J = \bar{A}_1 \times \cdots \times \bar{A}_t$ — разложение $\bar{A}$ в прямое произведение неразложимых колец $\bar{A}_1, \ldots, \bar{A}_t$ и $\bar{1} = \bar{f}_1 + \ldots + \bar{f}_t$ — соответствующее разложение $\bar{1} \in \bar{A}$ в сумму взаимно ортогональных идемпотентов.

Следуя [31], идемпотенты $\bar{f}_1, \ldots, \bar{f}_t$ можно поднимать по модулю J с сохранением ортогональности: $1 = f_1 + \ldots + f_t$, где $f_i f_j = \delta_{ij} f_j$ и $\bar{f}_i = f_i + J$ $(i,j = 1, \ldots, t)$.

Пусть $A_{ij} = f_i A f_j$ и $J_i = f_i J f_i$ $(i,j = 1, \ldots, t)$. Тогда имеем следующее двустороннее пирсовское разложение A и J:

$$A = \begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1t} \\ A_{21} & A_{22} & \ldots & A_{2t} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ A_{t1} & A_{t2} & \ldots & A_{tt} \end{pmatrix}, \qquad J = \begin{pmatrix} J_1 & A_{12} & \ldots & A_{1t} \\ A_{21} & J_2 & \ldots & A_{2t} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ A_{t1} & A_{t2} & \ldots & J_t \end{pmatrix}.$$

Лемма 3.3. *Если J — двусторонний правый T-нильпотентный идеал кольца A, то eJe — правый T-нильпотентный идеал кольца eAe для каждого ненулевого идемпотента $e \in A$.*

Теорема 3.4 (см. [29])**.** *Для кольца A с T-нильпотентным идеалом J следующие условия эквивалентны*:

1) *A неразложимо*;
2) *факторкольцо A/J^2 неразложимо.*

Пусть Q — конечный ориентированный граф (колчан в терминологии Габриэля). Через VQ обозначим множество всех вершин, а через AQ — множество всех стрелок колчана Q. Будем писать $Q = \{VQ, AQ\}$. Колчан Q_1 с $VQ_1 \subseteq VQ$ и $AQ_1 \subseteq AQ$ называется *подколчаном* колчана Q. Пусть Q_1 и Q_2 — подколчаны колчана Q. Будем говорить, что подколчан Q_1 содержит подколчан Q_2 и писать $Q_2 \subseteq Q_1$, если $VQ_2 \subseteq VQ_1$ и $AQ_2 \subseteq AQ_1$. *Путь колчана Q* из вершины i в вершину j — это упорядоченное множество k стрелок $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ таких, что начало каждой стрелки σ_m совпадает с концом предыдущей σ_{m-1} для $1 < m \leqslant k$; более того, вершина i — начало стрелки σ_1, в то время как вершина j — конец стрелки σ_k.

Определение 3.5. Колчан называется *сильно связным*, если существует путь между любыми двумя вершинами. Одноточечный граф без стрелок будем считать сильно связным колчаном.

Определение 3.6. Максимальный (по включению) сильно связный подколчан колчана Q называется *сильно связной компонентой*.

Определение 3.7. Разбиение множества вершин колчана Q на непересекающиеся подмножества такие, что подколчаны, соответствующие этим подмножествам, являются сильно связными колчанами (сильно связными компонентами колчана Q), будем называть *разбиением колчана Q* на сильно связные компоненты $Q_1, Q_2, \ldots, Q_m$ и обозначать $P(Q, Q_1, \ldots, Q_m)$.

Теорема 3.8 (см. [26, с. 231]). *Каждый колчан Q имеет разбиение $P(Q, Q_1, \dots, Q_m)$ на сильно связные компоненты Q_1, $Q_2, \dots, Q_m$. Это разбиение единственно с точностью до нумерации вершин колчана Q, т.е. если $P(Q, Q_1, \dots, Q_m)$ и $P(Q, G_1, \dots, G_n)$ — два таких разбиения, то $m = n$ и существует подстановка σ множества $\{1, 2, \dots, m\}$ такая, что $Q_i = G_{\sigma(i)}$ для $i = 1, 2, \dots, m$.*

Определение 3.9. Пусть $P(Q, Q_1, \dots, Q_m)$ — разбиение колчана Q на сильно связные компоненты $Q_1, \dots, Q_m$. *Конденсация* Q^* колчана Q — это колчан, вершины которого суть точки $q_1, \dots, q_m$, соответствующие сильно связным компонентам $Q_1, \dots, Q_m$; более того, стрелка с началом в вершине q_i и концом в q_j существует тогда и только тогда, когда в Q есть стрелка с началом в вершине, которая содержится в VQ_i и вершина с концом стрелки находится в VQ_j ($i \neq j$, $i, j = 1, 2, \dots, m$).

Пусть $P(PQ(A), Q_1, \dots, Q_m)$ — разбиение колчана $PQ(A)$ на сильно связные компоненты $Q_1, \dots, Q_m$. Будем говорить, что идемпотент f_k содержится в Q_i и писать $f_k \in Q_i$, если $k \in Q_i$.

Обозначим через g_i сумму всех $f_k \in Q_i$. Из предложения 2.5 и теоремы 3.8 следует, что $1 \in A$ разлагается: $1 = g_1 + \dots + g_m$, где $g_i g_j = \delta_{ij} g_j$ для $i, j = 1, \dots, m$.

Пусть $A = \bigoplus\limits_{i,j=1}^{m} g_i A g_j$ — двустороннее пирсовское разложение кольца A относительно разложения $1 = g_1 + \dots + g_m$.

Теорема 3.10 (см. [9]). *Пусть A — кольцо с конечной разложимой диагональю и T-нильпотентным первичным радикалом $\Pr(A)$. Существует двусторонний идеал $Y \subset \Pr(A)$ в A такой, что колчан $Q(A, Y)$ совпадает с конденсацией первичного колчана $PQ(A)$ колчана A.*

Доказательство. Предположим, что матрица смежности $[PQ(A)]$ первичного колчана $PQ(A)$ имеет вид

$$[PQ(A)] = \begin{pmatrix} [Q_1] & * & \dots & * \\ 0 & [Q_2] & \dots & * \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & [Q_m] \end{pmatrix}, \tag{1}$$

$Q_1, \dots, Q_m$ — сильно связные компоненты первичного колчана $PQ(A)$. Из теоремы 2.8 и предложения 2.5 следует, что $g_i A g_j = 0$ для $j < i$. Таким образом,

$$\Pr^2(A) = \begin{pmatrix} \Pr^2(g_1 A g_1) & * & \dots & * \\ 0 & \Pr^2(g_2 A g_2) & \dots & * \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \Pr^2(g_m A g_m) \end{pmatrix}. \tag{2}$$

Обозначим через Y двусторонний идеал кольца A, порожденный $\sum\limits_{i,j=1}^{m} g_i A g_j$ ($i \neq j$). Очевидно, $Y \subset \Pr(A)$ и

$$A/Y = g_1 A g_1 \times \dots \times g_m A g_m.$$

Из формул (1) и (2) следует, что $PQ(g_k A g_k) = Q_k$ для $k = 1$. Следовательно, все кольца $g_k A g_k$ неразложимы.

Можно поставить в соответствие вершинам колчана $Q(A, Y)$ числа $1, \dots, m$, которые соответствуют идемпотентам $g_1, \dots, g_m$. Очевидно, в колчане $Q(A, Y)$ имеется стрелка из i в j тогда и только тогда, когда имеется стрелка из i в j в конденсации $PQ(A)^*$ первичного колчана $PQ(A)$ кольца A. Следовательно, $Q(A, Y) = PQ(A)^*$. Теорема доказана. □

4. Колчан Пирса полусовершенного кольца

Пусть A — полусовершенное кольцо, R — его радикал Джекобсона. Предположим, что $e_1, \dots, e_r$ — попарно ортогональные локальные идемпотенты, соответствующие различным главным (т.е. неразложимым проективным) правым A-модулям $P_i = e_i A$ ($i = 1, \dots, r$).

Определение 4.1. *Колчан Пирса* полусовершенного кольца A — это ориентированный граф $\Gamma(A) = (V, E)$, множество вершин которого $V = \{e_1, \ldots, e_r\}$ и множество стрелок $E = \{(e_i, e_j) \mid e_i R e_j \neq 0\}$.

Замечание. Понятие колчана Пирса впервые появилось в [34, 37].

Очевидно, что колчан $\Gamma(A)$ не меняется при переходе к кольцам, эквивалентным в смысле Мориты. Напомним, что конечномерная алгебра A над полем k называется *алгеброй конечного типа*, если она имеет конечное число неэквивалентных неразложимых представлений. Заметим, что если A — алгебра конечного типа с нулевым квадратом радикала, то ее колчан Габриэля $Q(A)$ совпадает с колчаном Пирса $\Gamma(A)$. В общем случае это неверно, как можно видеть из следующих примеров.

Примеры. 1. Пусть $\mathbb{Z}_p$ — кольцо p-целых чисел и $\mathbb{Q}$ — поле рациональных чисел. Рассмотрим кольцо

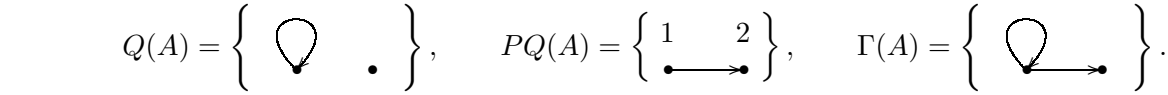
$$A = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}.$$

Тогда

$$\operatorname{rad} A = R = \begin{pmatrix} p\mathbb{Z}_p & \mathbb{Q} \\ 0 & 0 \end{pmatrix}, \qquad \Pr(A) = \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix}.$$

Для этого кольца

$$Q(A) = \left\{ \quad \right\}, \qquad PQ(A) = \left\{ \quad \right\}, \qquad \Gamma(A) = \left\{ \quad \right\}.$$

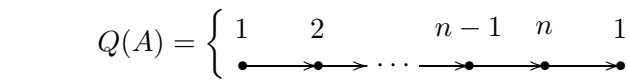


2. Пусть $\mathscr{O}$ — дискретно нормированное кольцо (не обязательно коммутативное) с телом частных D и единственным максимальным идеалом $\mathscr{M}$. Рассмотрим кольцо $(s \times s)$-матриц вида

$$A = H_s(\mathscr{O}) = \begin{pmatrix} \mathscr{O} & \mathscr{O} & \ldots & \mathscr{O} \\ \mathscr{M} & \mathscr{O} & \ldots & \mathscr{O} \\ \ldots\ldots\ldots\ldots\ldots & & & \\ \mathscr{M} & \mathscr{M} & \ldots & \mathscr{O} \end{pmatrix}.$$

В этом случае

$$Q(A) = \left\{ \quad \right\}, \qquad PQ(A) = \left\{ \quad \right\},$$



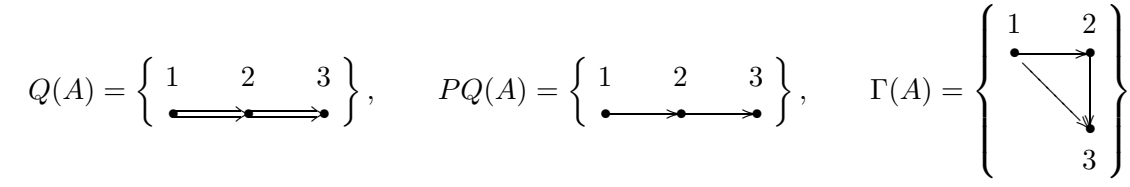
и $\Gamma(A)$ — полный граф на s вершинах, т.е. из каждой вершины $\Gamma(A)$ в каждую вершину $\Gamma(A)$ ведет стрелка и в каждой вершине ориентированного графа $\Gamma(A)$ есть петля.

3. Пусть $\mathbb{R}$, $\mathbb{C}$ — поля действительных и комплексных чисел соответственно. Рассмотрим кольцо вида

$$A = \begin{pmatrix} \mathbb{R} & \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{R} & \mathbb{C} \\ 0 & 0 & \mathbb{R} \end{pmatrix}.$$

В этом случае

$$Q(A) = \left\{ \quad \right\}, \qquad PQ(A) = \left\{ \quad \right\}, \qquad \Gamma(A) = \left\{ \quad \right\}$$



Переформулируем определение колчана $\Gamma(A)$ полусовершенного кольца A в терминах главных правых A-модулей $P_1, P_2, \ldots, P_r$. Пусть $A = P_1^{n_1} \oplus \ldots \oplus P_r^{n_r}$ — разложение полусовершенного кольца A в прямую сумму правых главных A-модулей. Более того, пусть $1 = f_1 + \ldots + f_r$ — соответствующее разложение единицы $1 \in A$ в сумму попарно ортогональных идемпотентов, т.е. $f_i A = P_i^{n_i}$

$(i = 1, \ldots, r)$, и модули $P_1, \ldots, P_r$ являются попарно неизоморфными. Принимая во внимание, что $\mathrm{Hom}(eA, fA) \simeq fAe$, легко видеть, что колчан $\Gamma(A)$ может быть определен как множество вершин $1, \ldots, s$, поставленных в соответствие модулям $P_1, \ldots, P_s$ (или идемпотентам $f_1, \ldots, f_s$), и множество стрелок такое, что из i в j идет стрелка $(i \neq j)$ тогда и только тогда, когда $\mathrm{Hom}(P_j, P_i) \neq 0$, и имеется петля в вершине i тогда и только тогда, когда $\mathrm{Hom}(P_i, P_iR) \neq 0$.

Теорема 4.2 (см. [7, с. 449])**.** *Полусовершенное кольцо A неразложимо тогда и только тогда, когда колчан $\Gamma(A)$ связен.*

Следующую теорему можно рассматривать как одну из версий теоремы Веддербарна—Артина.

Теорема 4.3. *Для полусовершенного кольца A следующие условия равносильны*:

1) *кольцо A является артиновым полупростым кольцом*;
2) *колчан Пирса $\Gamma(A)$ является конечным множеством точек.*

Доказательство. 1) $\Rightarrow$ 2) следует из определения колчана $\Gamma(A)$.

2) $\Rightarrow$ 1). Имеем $e_iRe_j = 0$ для локальных идемпотентов e_i и e_j из A. Тогда $R = 0$. Хорошо известно, что полусовершенное кольцо A с $R = 0$ zdkztncz полупростым артиновым. □

5. Колчаны полусовершенных полудистрибутивных колец

Напомним, что модуль M называется дистрибутивным, если для любых подмодулей K, L, N

$$K \cap (L + N) = K \cap L + K \cap N.$$

Ясно, что любой подмодуль и фактормодуль дистрибутивного модуля является дистрибутивным. Модуль называется полудистрибутивным, если он является прямой суммой дистрибутивных модулей. Кольцо называется правым (левым) полудистрибутивным, если оно является правым (левым) полудистрибутивным модулем над самим собой. Правое и левое полудистрибутивное кольцо называется полудистрибутивным.

Будем использовать термин «$SPSD$-кольцо» для полусовершенного полудистрибутивного кольца.

Теорема 5.1 (см. [18])**.** *Модуль является дистрибутивным тогда и только тогда, когда цоколь каждого его фактормодуля содержит не более одного экземпляра каждого простого модуля.*

Кольцо A называется полупервичным, если факторкольцо A/R артиново и R нильпотентен.

Теорема 5.2. *Полупервичное правое полудистрибутивное кольцо A является правым артиновым.*

Доказательство немедленно вытекает из теоремы 5.1.

Благодаря теореме 5.2 колчаны определены для произвольных $SPSD$-колец.

Теорема 5.3. *Для артинова кольца A такого, что квадрат его радикала Джекобсона равен нулю, следующие условия равносильны*:

1) *кольцо A полудистрибутивно*;
2) *из каждой точки колчана $Q(A)$ в другую (возможно, ту же самую) идет не более одной стрелки и левый колчан $Q'(A)$ получается из $Q(A)$ изменением направления всех стрелок.*

Определение 5.4. Полусовершенное кольцо A такое, что факторкольцо A/R^2 артиново, называется *Q-симметричным*, если левый колчан $Q'(A)$ получается из правого колчана $Q(A)$ изменением направления всех стрелок.

Из теоремы 5.3 следует, что каждое $SPSD$-кольцо Q-симметрично.

Определение 5.5. Колчан Q без кратных стрелок и кратных петель называется *простым*, т.е. Q является простым колчаном тогда и только тогда, когда его матрица смежности $[Q]$ является $(0,1)$-матрицей.

Следствие 5.6. *Колчан $Q(A)$ произвольного $SPSD$-кольца A является простым, т.е.* $Q_u(A) = Q(A)$.

Напомним, что полумаксимальное кольцо A — это полусовершенное полупервичное нетерово справа кольцо A такое, что для любого локального идемпотента $e \in A$ кольцо eAe является дискретно нормированным кольцом (не обязательно коммутативным). В [2] дано описание таких колец.

Теорема 5.7. *Каждое полумаксимальное кольцо изоморфно конечному прямому произведению первичных колец вида*

$$\Lambda = \begin{pmatrix} \mathscr{O} & \pi^{\alpha_{12}}\mathscr{O} & \dots & \pi^{\alpha_{1n}}\mathscr{O} \\ \pi^{\alpha_{21}}\mathscr{O} & \mathscr{O} & \dots & \pi^{\alpha_{2n}}\mathscr{O} \\ \dots & \dots & \dots & \dots \\ \pi^{\alpha_{n1}}\mathscr{O} & \pi^{\alpha_{n2}}\mathscr{O} & \dots & \mathscr{O} \end{pmatrix}, \tag{3}$$

где $n \geqslant 1$, $\mathscr{O}$ — дискретно нормированное кольцо с простым элементом π, α_{ij} — целые числа такие, что $\alpha_{ij} + \alpha_{jk} \geqslant \alpha_{ik}$ для всех i, j, k ($\alpha_{ii} = 0$ для любых i).

Кольцо $\mathscr{O}$ вкладывается в классическое тело частных $\mathscr{D}$, и (3) обозначает множество всех матриц $(a_{ij}) \in M_n(\mathscr{D})$ таких, что $a_{ij} \in \pi^{\alpha_{ij}}\mathscr{O} = e_{ii}\Lambda e_{jj}$, где $e_{11}, \dots, e_{nn}$ — матричные единицы кольца $M_n(\mathscr{D})$. Тогда Λ является черепичным порядком над дискретно нормированным кольцом (d.v.r.) [27, 39]. Очевидно, черепичный порядок Λ над дискретно нормированным кольцом $\mathscr{O}$ является нетеровым слева. Ясно, что $M_n(\mathscr{D})$ — классическое кольцо частных Λ.

Следующая теорема является *теоремой разложения* для полупервичных $SPSD$-колец.

Теорема 5.8 (см. [10])**.** *Для полусовершенного полупервичного нетерова справа кольца A следующие условия равносильны*:

1) *кольцо A является полудистрибутивным*;
2) *кольцо A является прямым произведением полупростого артинова кольца и полумаксимального кольца.*

Теорема 5.9 (см. [7, с. 454])**.** *Колчан $Q(A)$ нетерова полупервичного полусовершенного неразложимого кольца A сильно связен.*

Черепичные порядки над дискретно нормированными кольцами — это в точности нетеровы (но неартиновы) первичные $SPSD$-кольца. Таким образом, в нашей терминологии черепичный порядок — это первичное нетерово $SPSD$-кольцо с ненулевым радикалом Джекобсона.

Определение 5.10. Обозначим через $M_n(\mathbb{Z})$ кольцо всех квадратных $(n \times n)$-матриц над кольцом целых чисел $\mathbb{Z}$. Пусть $\mathscr{E} \in M_n(\mathbb{Z})$. Будем называть матрицу $\mathscr{E} = (\alpha_{ij})$ *матрицей показателей*, если

$$\alpha_{ij} + \alpha_{jk} \geqslant \alpha_{ik} \quad \text{для } i, j, k = 1, \dots, n, \qquad \alpha_{ii} = 0 \quad \text{для } i = 1, \dots, n.$$

Матрица $\mathscr{E}$ называется *приведенной матрицей показателей*, если

$$\alpha_{ij} + \alpha_{ji} > 0 \quad \text{для } i, j = 1, \dots, n.$$

Будем использовать следующие обозначения: $\Lambda = \{\mathscr{O}, \mathscr{E}(\Lambda)\}$, где $\mathscr{E}(\Lambda) = (\alpha_{ij})$ — матрица показателей кольца Λ, т.е. $\Lambda = \sum\limits_{i,j=1}^{n} e_{ij}\pi^{\alpha_{ij}}\mathscr{O}$, где e_{ij} — матричные единицы. Если черепичный порядок *приведенный*, то $\alpha_{ij} + \alpha_{ji} > 0$ для $i, j = 1, \dots, n$, $i \neq j$, т.е. $\mathscr{E}(\Lambda)$ — приведенная.

Пусть I — двусторонний идеал черепичного порядка Λ. Очевидно, $I = \sum\limits_{i,j=1}^{n} e_{ij}\pi^{\mu_{ij}}\mathscr{O}$, где e_{ij} — матричные единицы. Обозначим через $\mathscr{E}(I) = (\mu_{ij})$ матрицу показателей идеала I. Предположим, что I и J — двусторонние идеалы кольца Λ, $\mathscr{E}(I) = (\mu_{ij})$ и $\mathscr{E}(J) = (\nu_{ij})$. Легко видеть, что $\mathscr{E}(IJ) = (\delta_{ij})$, где $\delta_{ij} = \min\limits_{k}\{\mu_{ik} + \nu_{kj}\}$.

Теорема 5.11 (см. [19, 36]). *Колчан $Q(\Lambda)$ черепичного порядка Λ над дискретно нормированным кольцом $\mathscr{O}$ является сильно связным и простым. Если Λ приведенный, то*

$$Q(\Lambda) = \mathscr{E}(R^2) - \mathscr{E}(R).$$

Определение 5.12. Правый (соответственно, левый) Λ-модуль M (соответственно, N) называется правой (соответственно, левой) Λ-решеткой, если M (соответственно, N) — конечно порожденный свободный $\mathscr{O}$-модуль.

Например, все конечно порожденные проективные Λ-модули являются Λ-решетками.

Для черепичного порядка Λ обозначим через $\mathrm{Lat}_r(\Lambda)$ (соответственно, $\mathrm{Lat}_l(\Lambda)$) категорию правых (соответственно, левых) Λ-решеток. Обозначим через $S_r(\Lambda)$ (соответственно, $S_l(\Lambda)$) частично упорядоченное по включению множество, которое образовано всеми Λ-решетками, содержащимися в фиксированном простом правом $M_n(\mathscr{D})$-модуле W (соответственно, в простом левом $M_n(\mathscr{D})$-модуле V). Такие Λ-решетки называются неприводимыми.

Пусть $\Lambda = \{\mathscr{O}, \mathscr{E}(\Lambda)\}$ — черепичный порядок, W (соответственно, V) — простой правый (соответственно, левый) $M_n(\mathscr{D})$-модуль с $\mathscr{D}$-базисом $e_1, \ldots, e_n$ таким, что $e_ie_{jk} = \delta_{ij}e_k$ ($e_{ij}e_k = \delta_{jk}e_i$). Тогда правая (соответственно, левая) неприводимая Λ-решетка M (соответственно, N), лежащая в W (соответственно, в V) является Λ-модулем с $\mathscr{O}$-базисом $(\pi^{\alpha_1}e_1, \ldots, \pi^{\alpha_n}e_n)$, причем

$$\begin{cases} \alpha_i + \alpha_{ij} \geqslant \alpha_j & \text{в правом случае,} \\ \alpha_{ij} + \alpha_j \geqslant \alpha_i & \text{в левом случае.} \end{cases} \tag{4}$$

Следовательно, неприводимые Λ-решетки M могут быть отождествлены с целочисленным вектором $(\alpha_1, \ldots, \alpha_n)$, который удовлетворяет соотношениям (4). Будем писать $[M] = (\alpha_1, \ldots, \alpha_n)$ или $M = (\alpha_1, \ldots, \alpha_n)$.

Отношение порядка на множестве таких векторов и операции на нем, соответствующие сумме и пересечению неприводимых решеток, очевидны.

Замечание. Легко видеть, что неприводимые Λ-решетки $M_1 = (\alpha_1, \ldots, \alpha_n)$ и $M_2 = (\beta_1, \ldots, \beta_n)$ изоморфны тогда и только тогда, когда $\alpha_i = \beta_i + z$ для $i = 1, \ldots, n$ и $z \in \mathbb{Z}$.

Предложение 5.13. *Частично упорядоченные множества $S_r(\Lambda)$ и $S_l(\Lambda)$ являются антиизоморфными дистрибутивными решетками.*

Доказательство. Так как Λ — полудистрибутивное кольцо, то $S_r(\Lambda)$ (соответственно, $S_l(\Lambda)$) является дистрибутивной решеткой (см. [17]) относительно суммы и пересечения подмодулей.

Пусть $M = (\alpha_1, \ldots, \alpha_n) \in S_r(\Lambda)$. Тогда имеем $M^* = (-\alpha_1, \ldots, -\alpha_n)^T \in S_l(\Lambda)$. Если $N = (\beta_1, \ldots, \beta_n)^T \in S_l(\Lambda)$, то $N^* = (-\beta_1, \ldots, -\beta_n) \in S_r(\Lambda)$.

Очевидно, операция $*$ удовлетворяет следующим условиям:

1) $M^{**} = M$,
2) $(M_1 + M_2)^* = M_1^* \cap M_2^*$,
3) $(M_1 \cap M_2)^* = M_1^* + M_2^*$

в правом случае и аналогичным условиям в левом случае. Таким образом, отображение $* : S_r(\Lambda) \to S_l(\Lambda)$ является антиизоморфизмом. □

Замечание. Отображение $*$ определяет дуальность для неприводимых Λ-решеток.

Если $M_1 \subset M_2$, $M_1, M_2 \in S_r(\Lambda)$, то $M_2^* \subset M_1^*$. В этом случае Λ-решетка M_2 называется сверхмодулем Λ-решетки M_1 (соответственно, M_1^* является сверхмодулем M_2^*).

Определение 5.14 (см. [3]). Прямая сумма неприводимых Λ-решеток называется вполне разложимой Λ-решеткой.

Пусть $L = M_1 \oplus \cdots \oplus M_p$ — правая вполне разложимая Λ-решетка и $K = N_1 \oplus \ldots \oplus N_q$ — левая вполне разложимая Λ-решетка. Тогда $L^* = M_1^* \oplus \ldots \oplus M_p^*$ является левой вполне разложимой Λ-решеткой и $K^* = N_1^* \oplus \ldots \oplus N_q^*$ является правой вполне разложимой Λ-решеткой.

Черепичный порядок $\Lambda = \sum\limits_{i,j=1}^{n} e_{ij}\pi^{\alpha_{ij}}\mathscr{O}$ является вполне разложимой одновременно левой и правой Λ-решеткой, лежащей в $\tilde{\Lambda} = M_n(D)$.

Проективная Λ-решетка (т.е. конечно порожденный проективный Λ-модуль) является вполне разложимой Λ-решеткой.

Определение 5.15. Вполне разложимая Λ-решетка M называется *относительно инъективной*, если $M = P^*$, где P — проективная Λ-решетка.

Определение 5.16 (см. [6]). Черепичный порядок Λ называется горенштейновым черепичным порядком, если Λ_Λ^* является левой проективной Λ-решеткой.

Замечание. Очевидно, Λ_Λ^* является проективной левой Λ-решеткой тогда и только тогда, когда ${}_\Lambda\Lambda^*$ является проективной правой Λ-решеткой.

Теорема 5.17 (см. [6]). *Пусть $\Lambda = \{\mathscr{O}, \mathscr{E}(\Lambda) = (\alpha_{pq})\}$ — приведенный черепичный порядок. Тогда следующие условия равносильны*:

1) Λ *гореншетйнов*;
2) *существует подстановка $\sigma = \{i \to \sigma(i)\}$ такая, что $\alpha_{ik} + \alpha_{k\sigma(i)} = \alpha_{i\sigma(i)}$ для $i, k = 1, \ldots, n$.*

6. Колчаны полунаследственных $SPSD$-колец

Лемма 6.1 (см. [26, с. 194]). *Каждый ненулевой гомоморфизм между неразложимыми проективными модулями над полусовершенным полунаследственным кольцом является мономорфизмом.*

Кольца, удовлетворяющие этим условиям, называются *кусочными областями* [25].

Теорема 6.2 (см. [7]). *Первичный колчан $PQ(A)$ полусовершенной кусочной области A является ацикличным простым колчаном* (*т.е. не содержит ориентированных циклов*).

Теорема 6.3 (см. [30]). *Полунаследственное $SPSD$-кольцо A имеет классическое кольцо частных $\tilde{A}$.*

Теорема 6.4 (см. [30]). *Первичный колчан $PQ(A)$ полунаследственного $SPSD$-кольца A совпадает с колчаном $Q(\tilde{A})$ полунаследственного $SPSD$-кольца $\tilde{A}$.*

Определение 6.5 (см. [17]). Выражение «a *накрывает* b» в частично упорядоченом множестве P означает, что неравенства $a > x > b$ не выполняются ни для одного $x \in P$.

Определение 6.6. Пусть $P = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ — конечное частично упорядоченное множество с отношением порядка $\leqslant$. *Диаграмма* множества P — это колчан $Q(P)$ с множеством вершин $VQ(P) = \{1, \ldots, n\}$ и множеством стрелок $AQ(P)$ таким, что в $AQ(P)$ существует стрелка $\sigma : i \to j$ тогда и только тогда, когда α_j накрывает α_i.

Определение 6.7 (см. [34]). Колчан без ориентированных циклов называется *ацикличным колчаном*.

Очевидно, диаграмма частично упорядоченного множества является ацикличным простым колчаном.

Определение 6.8. Стрелка $\sigma : i \to j$ ацикличного колчана Q называется *лишней*, если существует путь из i в j длины, большей 1.

Теорема 6.9 (см. [26, с. 234])**.** *Пусть Q является ацикличным простым колчаном без лишних стрелок. Тогда Q является диаграммой некоторого конечного частично упорядоченного множества P. Обратно, диаграмма $Q(P)$ конечного частично упорядоченного множества P — это ациклический простой колчан без лишних стрелок.*

Частично упорядоченное множество $\mathscr{R} = \{a, b, c, d \mid a < b < d,\ a < c < d\}$ называется *ромбом*.

Теорема 6.10 (см. [30])**.** *Первичный колчан $PQ(A)$ полунаследственного $SPSD$-кольца A является диаграммой конечного частично упорядоченного множества без ромбов.*

Следующий пример показывает, что утверждение теоремы 6.4 неверно для кусочных $SPSD$-областей.

Пример. Пусть $\mathscr{O}$ — дискретно нормированное кольцо и $\mathscr{M}$ — его единственный максимальный идеал, $\mathscr{M} = \pi\mathscr{O} = \mathscr{O}\pi$. Рассмотрим кольцо

$$A = \begin{pmatrix} \mathscr{O} & \mathscr{O} & \mathscr{O} \\ 0 & \mathscr{O} & \pi\mathscr{O} \\ 0 & 0 & \mathscr{O} \end{pmatrix};$$

тогда

$$\tilde{A} = \begin{pmatrix} \mathscr{D} & \mathscr{D} & \mathscr{D} \\ 0 & \mathscr{D} & \mathscr{D} \\ 0 & 0 & \mathscr{D} \end{pmatrix}$$

— его классическое кольцо частных, где $\mathscr{D}$ тело частных кольца $\mathscr{O}$. Ясно, что

$$Q(\tilde{A}) = \Big\{ \bullet \longrightarrow \bullet \longrightarrow \bullet \Big\}.$$

Очевидно, кольцо A — это кусочная область, которая является $SPSD$-кольцом. Первичный радикал I кольца A имеет вид

$$I = \begin{pmatrix} 0 & \mathscr{O} & \mathscr{O} \\ 0 & 0 & \pi\mathscr{O} \\ 0 & 0 & 0 \end{pmatrix}.$$

Очевидно,

$$I^2 = \begin{pmatrix} 0 & 0 & \pi\mathscr{O} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad I/I^2 = \begin{pmatrix} 0 & \mathscr{O} & \mathscr{O}/\pi\mathscr{O} \\ 0 & 0 & \pi\mathscr{O} \\ 0 & 0 & 0 \end{pmatrix}.$$

Поэтому

$$PQ(A) = \left\{ \begin{array}{ccc} \bullet & \longrightarrow & \bullet \\ & \searrow & \downarrow \\ & & \bullet \end{array} \right\}$$

и $PQ(A) \neq Q(\tilde{A})$.

7. Матрицы показателей и их колчаны

Впервые $(0,1)$-порядки появились в [1] (см. также [2, 38]).

Определение 7.1. Черепичный порядок $\Lambda = \{\mathscr{O}, \mathscr{E}(\Lambda)\}$ называется $(0,1)$-*порядком*, если $\mathscr{E}(\Lambda)$ является $(0,1)$-матрицей.

Таким образом, под $(0,1)$-порядком будем всегда понимать черепичный $(0,1)$-порядок над дискретно нормированным кольцом $\mathscr{O}$.

Приведенному $(0,1)$-порядку Λ поставим в соответствие частично упорядоченное множество $P_\Lambda = \{1,\dots,n\}$ с отношением $\leqslant$, определяемым формулой $i \leqslant j \Leftrightarrow \alpha_{ij} = 0$. Очевидно, $(P,\leqslant)$ — это частично упорядоченное множество.

Обратно, с любым частично упорядоченным множеством $P = \{1,\dots,n\}$ свяжем приведенную $(0,1)$-матрицу $\mathscr{E}_p = (\lambda_{ij})$ следующим образом: $\lambda_{ij} = 0 \Leftrightarrow i \leqslant j$, и $\lambda_{ij} = 1$ в противном случае. Тогда $\Lambda(P) = \{\mathscr{O}, \mathscr{E}_P\}$ — приводимый $(0,1)$-порядок.

Определение 7.2. $(0,1)$-Матрица $\mathscr{E} \in (\mathbb{Z})$ называется $(0,1)$-*матрицей, ассоциированной с частично упорядоченным множеством* P, если она построена по следующему правилу: $\mathscr{E}(P) = (\lambda_{ij})$, где $\lambda_{ij} = 0$, $\Leftrightarrow i \leqslant j$ и $\lambda_{ij} = 1$ в противном случае. Такую $(0,1)$-матрицу будем обозначать $\mathscr{E}_P$.

Предложение 7.3. $(0,1)$-*Матрица* $\mathscr{E} \in M_n(\mathbb{Z})$ *является приведенной матрицей показателей тогда и только тогда, когда* $\mathscr{E} = \mathscr{E}_P$ *для некоторого конечного частично упорядоченного множества* P.

Доказательство. Если $\mathscr{E} \in M_n(\mathbb{Z})$ является приведенной $(0,1)$-матрицей показателей, то соотношение $\leqslant$, заданное формулой $i \leqslant j \Leftrightarrow \alpha_{ij} = 0$, определяет частичный порядок на множестве $\{1,\dots,n\}$. Это частично упорядоченное множество будем обозначать $P_{\mathscr{E}}$.

Действительно, $i \leqslant i$ для всех $i \in P_{\mathscr{E}}$; тогда $\lambda_{ii} = 0$.

Если $i \leqslant j$ и $j \leqslant k$, то $\alpha_{ij} + \alpha_{jk} \geqslant \alpha_{ik}$; таким образом, $0 \geqslant \alpha_{ik}$, т.е. $\alpha_{ik} = 0$ и $i \leqslant k$. Если $\alpha_{ij} = 0$ и $\alpha_{ji} = 0$, так как матрица $\mathscr{E}$ не имеет симметрических нулей, то $i = j$. Обратно, $\mathscr{E} = \mathscr{E}_{P_{\mathscr{E}}}$.

Обратно, пусть $\mathscr{E}_P$ — $(0,1)$-матрица, ассоциированная с конечным частично упорядоченным множеством $P = \{1,\dots,n\}$. Тогда $\alpha_{ii} = 0$ для $i = 1,\dots,n$. Покажем, что $\mathscr{E}_P$ не имеет симметрических нулей. Если $\alpha_{ij} = 0$ и $\alpha_{ji} = 0$, то $i = j$. Предположим, что хотя бы одно из α_{ij} и α_{jk} равно 1. Тогда кольцевые тождества $\alpha_{ij} + \alpha_{jk} \geqslant \alpha_{ik}$ выполняются автоматически. Таким образом, можно определить $\alpha_{ij} = \alpha_{jk} = 0$; тогда $i \leqslant k$, следовательно, $\alpha_{ik} = 0$, т.е. $\alpha_{ij} + \alpha_{jk} \geqslant \alpha_{ik}$. Итак, доказано, что $\mathscr{E}_P$ — приведенная $(0,1)$-матрица показателей. □

Приведем конструкцию, которая данному конечному частично упорядоченному множеству $P = \{p_1,\dots,p_n\}$ ставит в соответствие сильно связный колчан без кратных стрелок и кратных петель.

Обозначим через $P_{\max}$ (соответственно, $P_{\min}$) множество всех максимальных (соответственно, всех минимальных) элементов из P и через $P_{\max} \times P_{\min}$ — их декартово произведение.

Определение 7.4. Колчан $\tilde{Q}(P)$, полученный из диаграммы $Q(P)$ добавлением стрелок σ_{ij} для всех $(p_i, p_j) \in P_{\max} \times P_{\min}$, будем называть *колчаном, ассоциированным с частично упорядоченным множеством* P.

Очевидно, $\tilde{Q}(P)$ является сильно связным простым колчаном.

Теорема 7.5 (см. [19])**.** *Колчан* $Q(\Lambda(P))$ *совпадает с колчаном* $\tilde{Q}(P)$.

Определение 7.6. *Индекс* $\operatorname{in} P$ частично упорядоченного множества P — это максимальное действительное собственное значение матрицы смежности колчана $\tilde{Q}(P)$.

Определение 7.7 (см. [17])**.** Пусть X и Y — два (непересекающихся) частично упорядоченных множества. *Ординальная сумма* $X \oplus Y$ частично упорядоченных множеств X и Y — это множество всех $x \in X$ и $y \in Y$; $x < y$ для всех $x \in X$ и $y \in Y$; соотношения $x \leqslant x_1$ и $y \leqslant y_1$ $(x, x_1 \in X,$ $y, y_1 \in Y)$ остаются неизменными.

Ординальная сумма ассоциативна, и мы можем рассматривать ординальную степень $X^{\oplus n} = \underbrace{X \oplus \dots \oplus X}_{n}$ для любого частично упорядоченного множества X.

В частности, $CH_n = CH_1^{\oplus n}$ и $P_{2n} = ACH_2^{\oplus n}$, где $CH_1 = \{\bullet\}$ и $ACH_2 = \{\bullet \quad \bullet\}$. ACH_2 — это антицепь с двумя элементами.

Теорема 7.8 (см. [19]). *Приведенный $(0,1)$-порядок Λ горенштейнов тогда и только тогда, когда P_Λ является ординальной степенью одноточечного множества или антицепи из двух элементов.*

Теорема 7.9 (см. [19]). *Приведенный $(0,1)$-порядок Λ горенштейнов тогда и только тогда, когда $\operatorname{in} P_\Lambda = w(P_\Lambda) = 1$ или $\operatorname{in} P_\Lambda = w(P_\Lambda) = 2$. В первом случае Λ наследственно.*

Пусть $\mathscr{E} = (\alpha_{ij})$ — приведенная матрица показателей. Положим $\mathscr{E}^{(1)} = (\beta_{ij})$, где $\beta_{ij} = \alpha_{ij}$ для $i \neq j$ и $\beta_{ii} = 1$ для $i = 1, \ldots, n$, и $\mathscr{E}^{(2)} = (\gamma_{ij})$, где $\gamma_{ij} = \min\limits_{1 \leqslant k \leqslant n} (\beta_{ik} + \beta_{kj})$. Очевидно, $[Q] = \mathscr{E}^{(2)} - \mathscr{E}^{(1)}$ является $(0,1)$-матрицей. Таким образом, матрица $[Q]$ — это матрица смежности простого колчана $Q = Q(\mathscr{E})$.

Определение 7.10. Колчан $Q(\mathscr{E})$ будем называть *колчаном приведенной матрицы показателей $\mathscr{E}$*.

Определение 7.11. *Индекс* $\operatorname{in}\mathscr{E}$ приведенной матрицы показателей $\mathscr{E}$ — это максимальное действительное собственное значение матрицы смежности $[Q(\mathscr{E})]$ колчана $Q(\mathscr{E})$.

Определение 7.12. Приведенную матрицу показателей $\mathscr{E} = (\alpha_{ij}) \in M_n(\mathbb{Z})$ будем называть *горенштейновой*, если существует подстановка σ элементов $\{1, 2, \ldots, n\}$ такая, что $\alpha_{ik} + \alpha_{k\sigma(i)} = \alpha_{i\sigma(i)}$ для $i, k = 1, \ldots, n$.

Подстановку σ обозначим $\sigma(\mathscr{E})$. Заметим, что $\sigma(\mathscr{E})$ для приведенной горенштейновой матрицы показателей $\mathscr{E}$ не имеет циклов длины 1.

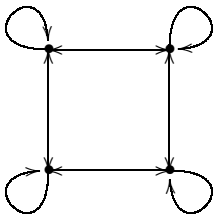
Пример. Таблица Кэли четверной группы Клейна $(2) \times (2)$ может быть записана в виде

$$K = K(4) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

Тогда $K(4)$ — это приведенная горенштейнова матрица показателей с подстановкой $\sigma = \sigma(K(4)) = (14)(23)$. Очевидно,

$$K^{(2)} = \begin{pmatrix} 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 \\ 3 & 3 & 2 & 2 \\ 3 & 3 & 2 & 2 \end{pmatrix}, \qquad [Q(K)] = K^{(2)} - K^{(1)} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} = 3 \cdot P_1,$$

где P_1 — дважды стохастическая матрица, и $Q(K)$ имеет вид



Очевидно, $\operatorname{in} K = 3$.

Определение 7.13 (см. [35, с. 140]). Квазигруппа Q такая, что $(xu)(vy) = (xv)(uy)$ для $x, y, u, v \in Q$, называется *энтропической*.

Пример (см. [35, с. 141]). Пусть $Q(5) = \{0, 1, 2, 3, 4\}$ — квазигруппа с таблицей Кэли

0	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

Ясно, что $Q(5)$ является энтропической квазигруппой. Таблица Кэли

$$\mathscr{E}(5) = \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}$$

квазигруппы $Q(5)$ — это приведенная горенштейнова матрица показателей с подстановкой $\sigma(\mathscr{E}(5)) = (12345)$. Очевидно,

$$[Q(\mathscr{E}(5))] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} = 2P_2,$$

где P_2 — дважды стохастическая матрица, и $\operatorname{in}\mathscr{E}(5) = 2$.

Определение 7.14. Приведенная горенштейнова матрица показателей $\mathscr{E}$ называется *циклической*, если $\sigma(\mathscr{E})$ — циклическая подстановка.

Теорема 7.15. *Пусть $\mathscr{E}$ — циклическая приведенная горенштейнова матрица показателей. Тогда $[Q(\mathscr{E})] = \lambda P$, где λ — положительное целое и P является дважды стохастической матрицей.*

Доказательство следует из [36, теорема 3.4].

8. Граф зацеплений полусовершенного кольца

Пусть $A_A = P_1^{n_1} \oplus \ldots \oplus P_s^{n_s}$ — разложение кольца A в прямую сумму неразложимых проективных модулей, где $P_1, \ldots, P_s$ — все, с точностью до изоморфизма, неразложимые правые проективные модули и $1 = f_1 + \ldots + f_s$ — соответствующее разложение $1 \in A$ в сумму попарно ортогональных идемпотентов, т.е. $P_i^{n_i} = f_i A$ для $i = 1, \ldots, s$; $A = \bigoplus\limits_{i,j=1}^{s} A_{ij}$, где $A_{ij} = f_i A f_j$ и $R = \bigoplus\limits_{i,j=1}^{s} f_i R f_j$, где $f_i R f_j = f_i A f_j$ для $i \neq j$.

Для $1 \leqslant k \leqslant s$ обозначим

$$M_k = P_1^{n_1} \oplus \ldots \oplus P_{k-1}^{n_{k-1}} \oplus (P_k R)^{n_k} \oplus P_{k+1}^{n_{k+1}} \oplus \ldots \oplus P_s^{n_s}.$$

Тогда $M_1, \ldots, M_s$ — максимальные (двусторонние) идеалы в A и $\bigcap\limits_{k=1}^{s} M_k = R$. Обратно, каждый максимальный (двусторонний) идеал M совпадает с некоторым M_k.

Поставим в соответствие идеалам $M_1, \ldots, M_s$ вершины $1, \ldots, s$ и соединим вершину i с вершиной j одной стрелкой тогда и только тогда, когда произведение $M_i M_j$ строго содержится в $M_i \cap M_j$.

Полученный простой колчан назовем *графом зацеплений* полусовершенного кольца A и обозначим $\mathscr{L}G(A)$ (см. [33]).

Пусть Q — колчан. Обозначим через Q_u колчан, полученный из Q заменой всех стрелок из i в j одной стрелкой (допускается случай $i = j$). Если в Q нет стрелок из i в j, то их нет и в Q_u.

Теорема 8.1. *Если A — нетерово справа полусовершенное кольцо, то $\mathscr{L}G(A) = Q_u(A)$.*

Доказательство. Легко видеть, что M_k имеет следующее двустороннее пирсовское разложение:

$$M_k = \begin{pmatrix} A_{11} & \dots & A_{1k} & \dots & A_{1s} \\ \dots & \dots & \dots & \dots & \dots \\ A_{k1} & \dots & R_{kk} & \dots & A_{ks} \\ \dots & \dots & \dots & \dots & \dots \\ A_{s1} & \dots & A_{sk} & \dots & A_{ss} \end{pmatrix}.$$

Рассмотрим $M_i \cap M_j$.

Случай $i = j$: $M_i \cap M_i = M_i$. Следовательно, петля в i-й вершине графа зацеплений $\mathscr{L}G(A)$ имеется тогда и только тогда, когда M_i^2 строго содержится в M_i. Очевидно, M_i^2 строго содержится в M_i тогда и только тогда, когда $f_iR^2f_i$ строго содержится в f_iRf_i. Таким образом, согласно Q-лемме существует петля в i-й вершине колчанов $Q(A)$ и $\mathscr{L}G(A)$ одновременно.

Случай $i < j$:

$$M_i \cap M_j = \begin{pmatrix} A_{11} & \dots & A_{1i} & \dots & A_{1j} & \dots & A_{1s} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_{i1} & \dots & R_{ii} & \dots & A_{ij} & \dots & A_{is} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_{j1} & \dots & A_{ji} & \dots & R_{jj} & \dots & A_{js} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_{s1} & \dots & A_{si} & \dots & A_{sj} & \dots & A_{ss} \end{pmatrix},$$

$$M_iM_j = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & R_{ii} & \dots & R_{ii}A_{ij} + A_{ij}R_{jj} + \sum\limits_{k \neq i} A_{ik}A_{kj} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & R_{jj} & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

Обратно, $f_iR^2f_j$ строго содержится в f_iRf_j тогда и только тогда, когда произведение M_iM_j строго содержится в $M_i \cap M_j$. Таким образом, согласно Q-лемме существует стрелка из i в j в колчанах $Q(A)$ и $\mathscr{L}G(A)$ одновременно.

Случай $i > j$ рассматривается аналогично. Теорема доказана. □

Замечание. В общем случае, если R — радикал Джекобсона полусовершенного кольца A, граф зацеплений $\mathscr{L}G(A)$ совпадает с колчаном $Q(A, R)$, ассоциированным с R.

Предложение 8.2. *Колчан $Q(A)$ полусовершенного полудистрибутивного кольца A совпадает с графом зацеплений $\mathscr{L}G(A)$.*

Доказательство вытекает из следствия 5.6 и теоремы 8.1.

Замечание. Из предложения 8.2 следует, что граф зацеплений черепичного порядка (см. [22]) совпадает с колчаном этого порядка.

9. Бирядные колчаны

Определение 9.1. Простой колчан Q называется *n-рядным*, если в каждой его вершине заканчивается по меньшей мере n стрелок и из каждой его вершины выходит по меньшей мере n стрелок.

Для $n = 1$ имеем определение полуцепного колчана и для $n = 2$ — определение для бирядного колчана.

Напомним определение полусовершенного бирядного кольца A (см. [8]).

Неразложимый A-модуль M называется *бирядным*, если M — дистрибутивный модуль, содержащий K_1 и K_2 (возможно, равные нулю) такие, что $K_1 + K_2$ — это M или наибольший собственный подмодуль в M и $K_1 \cap K_2$ — это или 0, или наименьший подмодуль в M, т.е. $\operatorname{soc} M$ является простым модулем.

Определение 9.2 (см. [8])**.** Полусовершенное кольцо A называется *бирядным*, если каждый правый и каждый левый неразложимый проективный A-модуль является бирядным.

Это понятие обобщает понятие бирядного артинова кольца, которое впервые было введено Фуллером [23].

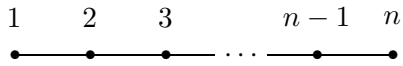
Теорема 9.3 (см. [11])**.** *Колчан $Q(A)$ полусовершенного бирядного кольца A является бирядным. Обратно, для любого бирядного колчана Q существует бирядная конечномерная алгебра A такая, что $Q(A) = Q$.*

Пусть A — полусовершенное кольцо и факторкольцо A/R^2 артиново справа. Тогда $Q(A) = Q(A/R^2)$. Определим колчан $RQ(A)$, который впервые появился в [24].

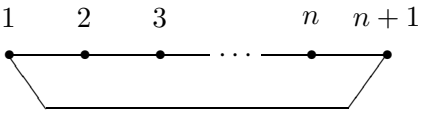
Пусть $VQ(A) = \{1, \ldots, n\}$ и существуют t_{ij} стрелок из вершины i в вершину j. Тогда $VRQ(A) = \{1, \ldots, n; \tau_1, \ldots, \tau_n\}$, т.е. число вершин $RQ(A)$ равно $2n$. $RQ(A)$ — это двудольный граф (существуют t_{ij} стрелок из вершины i в вершину τ_j). Если в $Q(A)$ нет стрелок из i в j, то в $RQ(A)$ нет стрелок из i в τ_j.

Замечание. Пусть Q — конечный ориентированный граф. Колчан, построенный из Q указанным выше способом, называется *производным колчаном* и обозначается RQ. Неориентированный граф $\overline{RQ}$, полученный из RQ снятием ориентации, будем называть *производным графом*.

Будем использовать следующие обозначения для таких двух типов неориентированных графов (см. [13, с. 242]): A_n ($n \geqslant 1$) для диаграмм Дынкина



и $\tilde{A}_n$ ($n \geqslant 1$) для диаграмм Евклида



Будем называть диаграмму Дынкина A_n цепью, а диаграмму Евклида $\tilde{A}_n$ — циклом.

Теорема 9.4 (см. [21])**.** *Для простого колчана следующие условия эквивалентны*:

1) *колчан Q является бирядным*;
2) *граф $\overline{RQ}$ является несвязным объединением цепей и циклов.*

Производный граф $\overline{RQ}$, где Q — бирядный колчан, называется *AB-графом* (см. [14]). Это простой двудольный граф с равными частями. AB-граф с n-вершинными частями называется *помеченным*, если вершины верхней части пронумерованы от 1 до n, а нижней — от $n+1$ до $2n$. Обозначим через $M_n^{(k)}$ число всех помеченных AB-графов с n-вершинными частями и в точности с k-элементными связными компонентами. M_n — число всех помеченных AB-графов. Очевидно, что $M_n = \sum\limits_{k=0}^{n} M_n^{(k)}$.

Теорема 9.5 (см. [14])**.**

$$\sum_{k=0}^{n} 2^k M_n^{(k)} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{n!}{(n-k)!} |IS_{n-k}|^2, \tag{5}$$

где $|IS_n|$ — число всех частичных (*т.е. не обязательно везде определенных*) *инъективных отображений n-элементного множества в себя.*

Так как $|IS_n| = \sum\limits_{i=0}^{n} \binom{n}{i}^2 \cdot i!$, то правая часть выражения (5) легко вычисляется, и это дает возможность получить верхнюю оценку для конкретного M_n. Эффективная нижняя оценка для M_n получена в [15]:

$$M_n > (n!)^2 \frac{n}{2}.$$

Теорема 9.6 (см. [14]). *Число B_n тех AB-графов с n-вершинными частями, все связные компоненты которых являются циклами, равно*

$$B_n = \sum_{\substack{(l_1,l_2,\ldots,l_n) \\ 1-l_1+2-l_2+\ldots+n-l_n=n}} \frac{(n!)^2}{(l_1!)^2 \cdot \prod\limits_{k=2}^{n} (2^{l_k} \cdot k^{l_k} \cdot l_k!)}.$$

Теорема 9.7 (см. [15]).

$$\lim_{n\to\infty} \frac{B_n}{M_n} = 0.$$

Следуя традиции использования выражения «почти все» (см., например, [12]), получаем следующее утверждение.

Следствие 9.8 (см. [15]). *Почти все AB-графы с n-вершинными частями содержат цепи.*

В заключение приведем значение величин B_n, M_n и B_n/M_n для малых n (см. [15]).

n	2	3	4	5
B_n	2	16	151	4991
M_n	16	256	7343	304186
B_n/M_n	0.125	0.0603773	0.0205638	0.0164077

Благодарность. Автор благодарен А. Ганюшкину за полезные обсуждения.

СПИСОК ЛИТЕРАТУРЫ

1. *Дрозд Ю. А., Кириченко В. В., Завадский А. Г.* Матричные задачи и интегральные представления// Изв. АН УССР. — 1974. — *38*, № 2. — С. 291–293.
2. *Завадский А. Г., Кириченко В. В.* Модули без кручения над простыми кольцами// Зап. науч. семин. ЛОМИ. — 1976. — *57*. — С. 100–116.
3. *Кириченко В. В.* Порядки, все представления которых вполне разложимы// Мат. заметки. — 1967. — *2*, № 2. — С. 139–144.
4. *Кириченко В. В.* Обобщенные унисериальные кольца/ Препринт № IM-75-1. — Киев, 1975.
5. *Кириченко В. В.* Обобщенные унисериальные кольца// Мат. сб. — 1976. — *99*, № 4. — С. 559–581.
6. *Кириченко В. В.* О квази-фробениусовых кольцах и порядках Гореншетйна// Тр. Мат. ин-та им. В. А. Стеклова АН СССР. — 1980. — *4*. — С. 171–177.
7. *Кириченко В. В., Валио С., Яременко Ю. В.* Полусовершенные кольца и их колчаны// в кн.: «Бесконечные группы и связанные с ними алгебраические стрктуры». — Киев: Ин-т математики НАН Украины, 1993. — С. 438–456.
8. *Кириченко В. В., Костюкевич П. П.* Бисериальые кольца// Укр. мат. ж. — 1986. — *38*, № 6. — С. 718–723.
9. *Кириченко В. В., Рябухин Ю. М.* Об идеале, ассоциированном с простым колчаном ассоциативного кольца// Изв. Гомельск. ун-та. — 2001. — *3*, № 6. — С. 53–56.
10. *Кириченко В. В., Хибина М. А.* Полусовершенные полудистрибутивные кольца// в кн.: «Бесконечные группы и связанные с ними алгебраические стрктуры». — Киев: Ин-т математики НАН Украины, 1993. — С. 457–480.
11. *Кириченко В. В., Яременко Ю. В.* Нетеровы бисериальные кольца// Укр. мат. ж. — 1988. — *40*, № 4. — С. 435–440.
12. *Коршунов А. Д.* Основные свойства случайных графов с большим числом вершин и ребер// Усп. мат. наук. — 1985. — *40*. — С. 107–173.

13. *Auslander M., Reiten I., Smalo S.* Representation theory of Artin algebras/ Cambridge Stud. Adv. Math. — Cambridge Univ. Press, 1995. — *36*.
14. *Avdeeva T. V., Ganyushkin O. G.* The number of quivers of Artinian biserial rings// Visnyk Kyiv. Univ., Ser. Phys.-Math. Sci. — 1999. — *3*. — С. 18–27.
15. *Avdeeva T. V., Ganyushkin O. G.* Almost all derivative quivers of Artinian biserial rings contain chains// Algebra Discr. Math. — 2003. — *1*. — С. 1–5.
16. *Bass H.* Finitistic dimension and homological generalization of semiprimary rings// Trans. Amer. Math. Sci. — 1960. — *95*. — С. 466–488.
17. *Birkhoff G.* Lattice Theory. — Providence: Amer. Math. Soc., 1973.
18. *Camillo V.* Distributive modules// J. Algebra. — 1975. — *36*. — С. 16–26.
19. *Chernousova Zh. T., Dokuchaev M. A., Kirichenko V. V., Khibina M. A., Miroshnichenko S. G., Zhuravlev V. N.* Tiled orders over discrete valuation rings, finite Markov chains, and partially ordered sets. I// Algebra Discr. Math. — 2002. — *1*. — С. 32–63.
20. *Chernousova Zh. T., Dokuchaev M. A., Kirichenko V. V., Khibina M. A., Miroshnichenko S. G., Zhuravlev V. N.* Tiled orders over discrete valuation rings, finite Markov chains, and partially ordered sets. II// Algebra Discr. Math. — 2003. — *2*. — С. 47–86.
21. *Danlyev Kh. M., Kirichenko V. V., Haletskaya Z. P., Yaremenko Yu. V.* Weakly prime semiperfect 2-rings and modules over them// Stud. Algebra. — Kiev: Math. Inst. Ukr. Akad. Nauk, 1995. — С. 5–32.
22. *Fujita H.* A remark on tiled orders over a local Dedekind domain// Tsukuba J. Math. — 1986. — *10*. — С. 121–130.
23. *Fuller K. R.* On generalization of serial rings. II// Commun. Algebra. — 1980. — *8*, № 7. — С. 635–661.
24. *Gabriel P.* Unzerlegbare Darstellungen. I// Manuscr. Math. — 1972. — *6*. — С. 71–103.
25. *Gordon R., Small L. W.* Piecewise domains// J. Algebra. — 1972. — *23*. — С. 553–564.
26. *Gubareni N. M., Kirichenko V. V.* Rings and modules. — Czestochowa, 2001.
27. *Jategaonkar V. A.* Global dimension of triangular orders over a discrete valuation ring// Proc. Amer. Math. Soc. — 1973. — *38*. — С. 8–14.
28. *Kasch F.* Modules and rings/ London Math. Soc. Monogr. — Academic Press, 1982. — *17*.
29. *Kirichenko V. V.* Decompositions of associative rings// *An. St. Univ. Ovidius Constanta*. — 2000. — *8*. — С. 53–62.
30. *Kirichenko V. V.* Semiperfect semidistributive rings// Algebras Representation Theory. — 2000. — *3*. — С. 81–98.
31. *Lambek J.* Lectures on rings and modules. — Waltham–Toronto–London: Blaisdell-Ginn, 1966.
32. *Müller B. J.* On semi-perfect rings// Ill. J. Math. — 1970. — *14*, № 3. — С. 464–467.
33. *Müller B. J.* Localization in fully bounded Noetherian rings// Pac. J. Math. — 1976. — *67*. — С. 233–245.
34. *Pierce R. S.* Associative algebras/ Grad. Texts Math. — Berlin–Heidelberg–New York: Springer-Verlag, 1982. — *88*.
35. *Plugfelder H. O.* Quasigroups and loops: Introduction. — Berlin: Heldermann, 1990.
36. *Roggenkamp K. W., Kirichenko V. V., Khibina M. A., Zhuravlev V. N.* Gorenstein tiled orders// Commun. Algebra. — 2001. — *29*. — С. 4231–4247.
37. *Rowen L. H.* Ring theory. Vol. I, II. — New York–Boston: Academic Press, 1988.
38. *Simson D.* Linear representations of partially ordered sets and vector categories/ Algebra Logic Appl. — Gordon and Breach, 1992. — *4*.
39. *Tarsy R. B.* Global dimension of orders// Trans. Amer. Math. Soc. — 1970. — *151*. — С. 335–340.

В. В. Кириченко
Киевский национальный университет им. Т. Шевченко
E-mail: vkir@univ.kiev.ua

Современная математика и ее приложения. Том 14 (2004). С. 40–47

УДК 512.554

ПРОМЕЖУТОЧНЫЙ РОСТ РАЗРЕШИМЫХ СУПЕРАЛГЕБР ЛИ

© 2004 г. **С. Г. КЛЕМЕНТЬЕВ, В. М. ПЕТРОГРАДСКИЙ**

Аннотация. Конечно порожденные разрешимые алгебры Ли имеют промежуточный рост, который находится между полиномиальным и экспоненциальным ростами. В. М Петроградским была предложена шкала классификации промежуточного роста алгебр Ли. Был вычислен рост разрешимых алгебр Ли $F(\mathbf{A}^q, k)$ с конечным числом порождающих k, которые свободны относительно фиксированной ступени разрешимости q. Позже применение производящих функций позволило найти более точную асимптотику. Эти результаты были получены в общности полинильпотентных алгебр Ли.

В настоящей работе рассматривается случай супералгебр Ли; формулируются основные результаты и описываются методы их доказательства. Цель — вычислить рост свободной разрешимой супералгебры Ли $F(\mathbf{A}^q, m, k)$ ступени q, порожденной m четными и k нечетными образующими. Доказательство опирается на точную формулу производящей функции для этой супералгебры, полученную ранее. Результат получен в общности свободных полинильпотентных супералгебр Ли.

СОДЕРЖАНИЕ

1. Введение

Зафиксируем основное поле K. Напомним, что $\mathbb{Z}_2$-градуированная алгебра Ли $L = L_+ \oplus L_-$ называется *супералгеброй Ли*, если она удовлетворяет следующим градуированным тождествам [28]. Пусть $\varepsilon(L_+, L_+) = \varepsilon(L_+, L_-) = \varepsilon(L_-, L_+) = 1$ и $\varepsilon(L_-, L_-) = -1$. Тогда

$$[x, y] = -\varepsilon(x, y)[y, x], \qquad x, y \in L_\pm \qquad \text{(антикоммутативность)};$$
$$[x, [y, z]] = [[x, y], z] - \varepsilon(y, z)[[x, z], y], \qquad x, y, z \in L_\pm \qquad \text{(тождество Якоби)}.$$

(Если $\operatorname{char} K = 2$, необходимы некоторые дополнительные условия [14]: в случае $\operatorname{char} K = 3$ полагаем также $[[y, y], y] = 0$ для всех $y \in L_-$; в других характеристиках это тождество автоматически выполняется). *Многообразием* (супер)алгебр (Ли) называют класс всех (супер)алгебр, удовлетворяющих некоторому фиксированному набору (градуированных или неградуированных) тождеств. О многообразиях алгебр Ли см. [1]. Супералгебры Ли и их многообразия изучаются также в [14, 21].

Пусть L — (супер)алгебра Ли. *Нижний центральный ряд* определяется итерированием $L^1 = L$, $L^{i+1} = [L, L^i]$, $i = 1, 2, \ldots$. Алгебра L называется *нильпотентной* класса s, если $L^{s+1} = \{0\}$, $L^s \neq \{0\}$. Все нильпотентные алгебры Ли класса s образуют многообразие, обозначаемое $\mathbf{N}_s$. Это обозначение также будем использовать для многообразий нильпотентных супералгебр Ли класса s. Напомним, что L *полинильпотентна* с последовательностью $(s_q, \ldots, s_2, s_1)$ если и только если существует цепочка идеалов $0 = L_{q+1} \subset L_q \subset \cdots \subset L_2 \subset L_1 = L$ такая, что $L_i/L_{i+1} \in \mathbf{N}_{s_i}$, $i = 1, \ldots, q$. Все полинильпотентные (супер)алгебры Ли с фиксированным набором $(s_q, \ldots, s_2, s_1)$ образуют многообразие, обозначаемое $\mathbf{N}_{s_q} \cdots \mathbf{N}_{s_2} \mathbf{N}_{s_1}$. В случае $s_q = \cdots = s_1 = 1$ получаем многообразие $\mathbf{A}^q$ *разрешимых* (супер)алгебр Ли ступени q. Полинильпотентные многообразия групп

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 01-01-00728) и фонда А. фон Гумбольдта.

и алгебр Ли и их взаимосвязь были рассмотрены А. Л. Шмелькиным [13]. Базис для свободной полинильпотентной алгебры Ли был построен Л. А. Бокутем [3], случай свободных разрешимых алгебр Ли рассмотрен в монографии К. Ройтенауера [27].

Рассмотрим супералгебру Ли L с разложением на четную и нечетную компоненты $L = L_+ \oplus L_-$. Свободную алгебру многообразия $\mathbf{M}$, порожденную X, обозначим через $F(\mathbf{M}, X)$, $X = X_+ \cup X_-$. Пусть $X_+ = \{x_i | i \in I_+\}$, $X_- = \{x_j | j \in I_-\}$. Напомним, что $F(\mathbf{M}, X)$ — это алгебра, порожденная X и такая, что для произвольной $H = H_+ \oplus H_- \in \mathbf{M}$ и любых $y_i \in H_+$, $i \in I_+$, $y_j \in H_-$, $j \in I_-$, существует гомоморфизм $\phi : F(\mathbf{M}, X) \to H$ такой, что $\phi(x_i) = y_i$, $i \in I_+ \cup I_-$. В случае $|X_+| = m$, $|X_-| = k$ также будем использовать обозначение $F(\mathbf{M}, X) = F(\mathbf{M}, m, k)$.

Легко проверить, что любая полинильпотентная (супер)алгебра Ли разрешима, т.е. лежит в некотором $\mathbf{A}^q$ для достаточно большого q. Поэтому, изучая свободные полинильпотентные (супер)алгебры Ли, мы, во-первых, изучаем некоторые разрешимые (супер)алгебры Ли, а во-вторых, случай свободных разрешимых (супер)алгебр Ли является частным случаем нашего исследования, так как $F(\mathbf{A}^q, X) = F(\underbrace{\mathbf{N}_1 \cdots \mathbf{N}_1}_{q \text{ раз}}, X)$.

Рассмотрим (ассоциативную или лиеву) алгебру A над полем K, порожденную конечным множеством X. Обозначим через $A^{(X,n)}$ подпространство, образованное всеми мономами из элементов множества X, длина которых не превышает n. Введем функции роста

$$\gamma_A(n) = \gamma_A(X, n) = \dim_K A^{(X,n)}, \qquad n \in \mathbb{N};$$
$$\lambda_A(n) = \gamma_A(n) - \gamma_A(n-1), \qquad n \in \mathbb{N}.$$

Здесь и далее $\dim_K$ обозначает размерность векторного пространства над полем K. Если A — ассоциативная алгебра с единицей, то мы полагаем, что единица принадлежит всем $A^{(X,n)}$, $n \geqslant 0$, и $\gamma_A(0) = \lambda_A(0) = 1$. На функциях $f : \mathbb{N} \to \mathbb{R}^+$, где $\mathbb{R}^+ = \{\alpha \in \mathbb{R} \,|\, \alpha > 0\}$, введем частичный порядок: $f(n) \overset{\text{a}}{\leqslant} g(n)$, если и только если существует $N > 0$, такое что $f(n) \leqslant g(n)$, $n \geqslant N$.

Рост, меньший любой экспоненты, называется *субэкспоненциальным*. Если он к тому же больше любого полиномиального роста, то его называют *промежуточным*. Для изучения таких видов роста была предложена следующая шкала функций [7, 22]. Введем обозначения

$$\ln^{(1)} n = \ln n; \quad \ln^{(q+1)} n = \ln(\ln^{(q)} n), \quad q = 1, 2, \ldots.$$

Рассмотрим последовательность функций $\Phi^q_\alpha(n)$, $q = 1, 2, 3, \ldots$, натурального аргумента с параметром $\alpha \in \mathbb{R}^+$:

$$\Phi^1_\alpha(n) = \alpha; \qquad q = 1;$$
$$\Phi^2_\alpha(n) = n^\alpha; \qquad q = 2;$$
$$\Phi^3_\alpha(n) = \exp(n^{\alpha/(\alpha+1)}); \qquad q = 3;$$
$$\Phi^q_\alpha(n) = \exp\left(\frac{n}{(\ln^{(q-3)} n)^{1/\alpha}}\right), \qquad q = 4, 5, \ldots.$$

Предположим, что $f(n)$ — положительно определенная функция натурального аргумента. Определим ее (*верхнюю*) *размерность уровня* q, $q = 1, 2, 3, \ldots$, и *нижнюю размерность уровня* q формулами

$$\operatorname{Dim}^q f(n) = \inf\{\alpha \in \mathbb{R}^+ \mid f(n) \overset{\text{a}}{\leqslant} \Phi^q_\alpha(n)\},$$
$$\underline{\operatorname{Dim}}^q f(n) = \sup\{\alpha \in \mathbb{R}^+ \mid f(n) \overset{\text{a}}{\geqslant} \Phi^q_\alpha(n)\}.$$

Рассмотрим конечно порожденную алгебру A. Определим *q-размерность* и *нижнюю q-размерность*, $q = 1, 2, 3, \ldots$, алгебры A следующим образом:

$$\operatorname{Dim}^q A = \operatorname{Dim}^q \gamma_A(n), \quad \underline{\operatorname{Dim}}^q A = \underline{\operatorname{Dim}}^q \gamma_A(n).$$

Грубо говоря, условие $\operatorname{Dim}^q A = \underline{\operatorname{Dim}}^q A = \alpha$ означает, что функция роста $\gamma_A(n)$ ведет себя как $\Phi^q_\alpha(n)$. Введенные q-размерности не зависят от порождающего множества X (см. [22]). Заметим, что 1-размерность соответствует размерности векторного пространства A над полем K. Размерности уровня 2 — это в точности верхняя и нижняя размерности Гельфанда—Кириллова (см. [16, 18, 20]). Размерности уровня 3 соответствуют суперразмерностям [15] с точностью до нормализации (см. [22]). Обозначим универсальную обертывающую алгебру (супер)алгебры Ли L через $U(L)$. Следующие две теоремы являются важными фактами, связывающие введенные понятия шкалы функций и q-размерностей.

Теорема 1.1 (см. [7, 22]). *Пусть L — конечно порожденная алгебра Ли и $\operatorname{Dim}^q L = \alpha > 0$, $q = 1, 2, \ldots$. Если $q \geqslant 3$, то также предположим, что $\underline{\operatorname{Dim}}^q L = \alpha$; если $q = 2$, то предполагаем, что $\underline{\operatorname{Dim}}^2 \lambda_L(n) = \alpha - 1$ и $\alpha \geqslant 1$. Тогда*

$$\underline{\operatorname{Dim}}^{q+1} U(L) = \operatorname{Dim}^{q+1} U(L) = \alpha.$$

А. Лихтман доказал, что рост конечно порожденных разрешимых алгебр Ли субэкспоненциален [19]. Следующий результат описывает рост таких алгебр с помощью введенной шкалы функций.

Теорема 1.2 (см. [22]). *Рассмотрим свободную полинильпотентную алгебру Ли*

$$L = F(\mathbf{N}_{s_q} \cdots \mathbf{N}_{s_2} \mathbf{N}_{s_1}, k)$$

ранга k, где $k \geqslant 2$, $q \geqslant 2$. Тогда

$$\underline{\operatorname{Dim}}^q L = \operatorname{Dim}^q L = s_2 \dim_K F(\mathbf{N}_{s_1}, k).$$

Как частный случай получаем следующее утверждение.

Следствие 1.1 (см. [7]). *Пусть $L = F(\mathbf{A}^q, k)$ — свободная разрешимая алгебра Ли ступени q и ранга k, где $k \geqslant 2$, $q \geqslant 1$. Тогда $\underline{\operatorname{Dim}}^q L = \operatorname{Dim}^q L = k$.*

Более точная асимптотика для свободных полинильпотентных алгебр Ли $L = F(\mathbf{N}_{s_q} \cdots \mathbf{N}_{s_1}, k)$ найдена в [23]. Этот результат также дал ответ на вопрос М. И. Каргаполова [6] о описании рангов факторов нижнего центрального ряда свободных полинильпотентных конечно порожденных групп. Ранее Г. П. Егорычевым была найдена точная рекурсивная формула [5]. Описав асимптотическое поведение этих рангов, В. М. Петроградский предложил новое решение этой проблемы [23]. Работа [23] в основном опирается на технику производящих функций и изучение их роста.

Обозначим через $\zeta(*)$, $\Gamma(*)$, $\mu(*)$ и $\delta_{i,j}$ дзета-функцию Римана, гамма-функцию, функцию Мебиуса и символ Кронекера соответственно.

2. Основной результат

Наша цель — изучение роста разрешимых *супер*алгебр Ли. Сформулируем первый результат в этом направлении. Оказывается, что $F(\mathbf{N}_{s_q} \cdots \mathbf{N}_{s_1}, m, k)$ также лежит, как правило, на уровне q.

Теорема 2.1. *Пусть $L = F(\mathbf{N}_{s_q} \cdots \mathbf{N}_{s_2} \mathbf{N}_{s_1}, m, k)$ — свободная полинильпотентная супералгебра Ли, где $m + k \geqslant 2$ и $q \geqslant 2$. Тогда*

1) $\underline{\operatorname{Dim}}^q L = \operatorname{Dim}^q L = s_2 \dim F_+(\mathbf{N}_{s_1}, m, k)$;
2) *условие $\dim F_+(\mathbf{N}_{s_1}, m, k) = 0$ эквивалентно $s_1 = 1$ и $m = 0$. Если в этом случае выполнено неравенство $q \geqslant 3$, то $\underline{\operatorname{Dim}}^{q-1} L = \operatorname{Dim}^{q-1} L = s_3 \dim F_+(\mathbf{N}_{s_2}\mathbf{A}, 0, k)$.*

Как частный случай, получаем следующее утверждение.

Следствие 2.1. *Пусть $L = F(\mathbf{A}^q, m, k)$ — свободная разрешимая супералгебра Ли ступени q, где $m + k \geqslant 2$, $q \geqslant 2$. Тогда*

1) $\underline{\operatorname{Dim}}^q L = \operatorname{Dim}^q L = m$;
2) *если $m = 0$ и $q \geqslant 3$, то $\underline{\operatorname{Dim}}^{q-1} L = \operatorname{Dim}^{q-1} L = 1 + (k-1)2^{k-1}$.*

Будем называть второй случай *вырожденным*. Сформулируем основной результат, из которого сразу вытекает теорема 2.1. Полные доказательства основных результатов см. в [17].

Теорема 2.2. *Рассмотрим полинильпотентное многообразие супералгебр Ли* $\mathbf{V} = \mathbf{N}_{s_q} \cdots \mathbf{N}_{s_1}$, $q \geqslant 2$. *Пусть* $L = F(\mathbf{V}, m, k)$ *— его свободная супералгебра, порожденная множеством* $X = X_+ \cup X_-$, $X_+ = \{x_1, \ldots, x_m\}$, $X_- = \{x_{m+1}, \ldots, x_{m+k}\}$. *Тогда справедливы следующие утверждения.*

1) *Если* $s_1 > 1$ *или* $m > 0$, *то*

$$\gamma_L(X,n) = \begin{cases} \dfrac{A+o(1)}{N!} n^N, & q = 2, \\ \exp\left((C+o(1)) n^{\frac{N}{N+1}}\right), & q = 3, \\ \exp\left((B^{1/N}+o(1)) \dfrac{n}{(\ln^{(q-3)} n)^{1/N}}\right), & q \geqslant 4, \end{cases}$$

где

$$N = s_2 \dim F_+(\mathbf{N}_{s_1}, m, k), \qquad A = \frac{1}{s_2}\left((m+k-1)\frac{2^{\dim F_-(\mathbf{N}_{s_1},m,k)}}{\prod\limits_{j=1}^{s_1} j^{\psi_+(j)}}\right)^{s_2},$$

$$B = s_3 A \zeta(N+1)\left(1 - \frac{1-\delta_{k,0}}{2^{N+1}}\right), \qquad C = \left(1+\frac{1}{N}\right)(BN)^{\frac{1}{1+N}},$$

а $\psi_+(j) = \dim F_{j,+}(\mathbf{N}_{s_1}, m, k)$ *— размерности четных частей однородных компонент, где* $1 \leqslant j \leqslant s_1$.

2) *Если* $s_1 = 1$, $m = 0$ *и* $q \geqslant 3$, *то*

$$\gamma_L(X,n) = \begin{cases} \dfrac{A+o(1)}{N!} n^N, & q = 3, \\ \exp\left((C+o(1)) n^{\frac{N}{N+1}}\right), & q = 4, \\ \exp\left((B^{1/N}+o(1)) \dfrac{n}{(\ln^{(q-4)} n)^{1/N}}\right), & q \geqslant 5, \end{cases}$$

где

$$N = s_3 \dim F_+(\mathbf{N}_{s_2}\mathbf{A}, 0, k), \qquad A = \frac{1}{s_3}\left((k-1)\frac{2^{\dim F_-(\mathbf{N}_{s_2}\mathbf{A},0,k)}}{\prod\limits_{2|j} j^{\phi(j)}}\right)^{s_3},$$

$$B = s_4 A \zeta(N+1)\left(1 - \frac{1}{2^{N+1}}\right), \qquad C = \left(1+\frac{1}{N}\right)(BN)^{\frac{1}{1+N}},$$

а $\phi(j) = \dim F_j(\mathbf{N}_{s_2}\mathbf{A}, 0, k)$ *— размерности однородных компонент конечномерной алгебры* $F(\mathbf{N}_{s_2}\mathbf{A}, 0, k)$.

Обращаем внимание, что найденная асимптотика роста верна только для стандартного порождающего множества X. Случай свободных разрешимых супералгебр Ли $L = F(\mathbf{A}^q, m, k)$, $q \geqslant 2$, является частным случаем приведенной теоремы и легко из нее выводится.

Основной результат доказывается с помощью техники производящих функций. Рассмотрим алгебру A, порожденную конечным множеством X и однородную относительно степени по X. Получаем $A = \bigoplus\limits_{n=0}^{\infty} A_n$ и $\dim A_n = \lambda_A(X, n)$. В этом случае можно определить ряд Гильберта—Пуанкаре

$$\mathscr{H}_X(A, t) = \sum_{n=0}^{\infty} \dim A_n t^n.$$

В следующем разделе будут введены некоторые другие ряды. Следующий результат играет важную роль в доказательстве, а также представляет самостоятельный интерес.

Теорема 2.3. *Рассмотрим полинильпотентное многообразие супералгебр Ли* $\mathbf{V} = \mathbf{N}_{s_q} \cdots \mathbf{N}_{s_1}$, $q \geqslant 2$. *Пусть* $L = F(\mathbf{V}, m, k)$, $m + k \geqslant 2$. *Тогда ряд Гильберта—Пуанкаре по отношению к стандартному порождающему множеству* X *растет следующим образом, где* $t \to 1 - 0$:

1) *если* $s_1 > 1$ *или* $m > 0$, *то*

$$\mathscr{H}_X(L, t) = \begin{cases} \dfrac{A + o(1)}{(1-t)^N}, & q = 2, \\ \exp^{(q-2)}\left(\dfrac{B + o(1)}{(1-t)^N}\right), & q \geqslant 3; \end{cases}$$

2) *если* $s_1 = 1$, $m = 0$ *и* $g \geqslant 3$, *то*

$$\mathscr{H}_X(L, t) = \begin{cases} \dfrac{A + o(1)}{(1-t)^N}, & q = 3, \\ \exp^{(q-3)}\left(\dfrac{B + o(1)}{(1-t)^N}\right), & q \geqslant 4. \end{cases}$$

Константы N, A *и* B *те же самые, что и в соответствующих случаях теоремы* 2.2.

3. Производящие функции для разрешимых супералгебр Ли

Как видно из теоремы 2.3, производящие функции и их рост играют важную роль в наших рассуждениях. В этом разделе будет сформулирована точная формула производящей функции для свободной разрешимой (полинильпотентной) супералгебры Ли (теорема 3.1). Доказательство основного результата опирается на эту формулу, которая, кроме того, относится к области перечислительной комбинаторики [4, 11, 30].

Пусть $X = \{x_i \mid i \in I\}$, где $I = I_+ \cup I_-$, — не более чем счетное порождающее множество для супералгебры $A = A_+ \oplus A_-$. Предположим, что A полиоднородна относительно X. Например, это имеет место для относительно свободной алгебры A некоторого многообразия супералгебр, где $X = X_+ \cup X_-$ — ее свободное порождающее множество. Обозначим $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Рассмотрим градуировку $A = \bigoplus\limits_{\alpha \in \mathbb{N}_0^I} A_\alpha$, заданную предположением $x_i \in A_{\alpha_i}$, где $\alpha_i = (\ldots, 0, 1, 0, \ldots) \in \mathbb{N}_0^I$ с 1 на i-м месте. Определим гомоморфизм $\varepsilon : \mathbb{N}_0^I \to \{\pm 1\}$, полагая $\varepsilon(\alpha_i) = \pm 1$ для $i \in I_\pm$. Последовательность $\alpha = \sum\limits_{i \in I} m_i \alpha_i \in \mathbb{N}_0^I$ имеет лишь конечное число ненулевых элементов m_i, поэтому можно определить $\mathbf{t}^\alpha = \prod\limits_{i \in I} t_i^{m_i}$. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[[\mathbf{t}]] = \mathbb{Q}[[t_i | i \in I]]$. Предположим, что $W = \bigoplus\limits_{\alpha \in \mathbb{N}_0^I} W_\alpha \subset A$ — однородная подалгебра; тогда ее ряд Гильберта—Пуанкаре определяется следующим образом:

$$\mathscr{H}_X(W, \mathbf{t}) = \mathscr{H}_X(W, t_i | i \in I) = \sum_{\alpha \in \mathbb{N}_0^I} \dim(W_\alpha)\, \mathbf{t}^\alpha \in \mathbb{Q}[[\mathbf{t}].$$

Далее будем использовать следующие операторы, действующие на кольце формальных степенных рядов $\mathbb{Q}[[\mathbf{t}]]$ (см. [9, 25]):

$$\begin{gathered}\phi^{[-]}(\mathbf{t}) = \phi\Big|_{t_i=\varepsilon(t_i)t_i,\ i\in I}; \qquad \phi^{[m]}(\mathbf{t}) = \phi\Big|_{t_i=\varepsilon(t_i)^{m+1}t_i^m,\, i\in I}, \quad m\in\mathbb{N};\\ \mathscr{E}(\phi)(\mathbf{t}) = \exp\left(\sum_{m=1}^{\infty}\frac{1}{m}\phi^{[m]}(\mathbf{t})\right) = \prod_{\alpha\in\mathbb{N}_0^I}(1-\varepsilon(\alpha)\mathbf{t}^\alpha)^{-\varepsilon(\alpha)b_\alpha},\end{gathered} \tag{1}$$

где

$$\phi(\mathbf{t}) = \sum_{\alpha\in\mathbb{N}_0^I} b_\alpha \mathbf{t}^\alpha \in \mathbb{Q}[[\mathbf{t}]]_0,$$

а $\mathbb{Q}[[\mathbf{t}]]_0$ обозначает множество рядов с нулевым свободным членом. Равенство (1) доказано в [9]. Для того, чтобы правая часть (1) была определена, предположим, что $b_\alpha \in \mathbb{Z}$. Такие ряды возникают при перечислении универсальных обертывающих алгебр [12]. Важность оператора $\mathscr{E}$ объясняется следующим фактом.

Лемма 3.1 (см. [9]). *Пусть L — супералгебра Ли, порожденная не более чем счетным порождающим множеством $X = X_+ \cup X_-$ и полиоднородная относительно него. Тогда ряд универсальной обертывающей алгебры равен $\mathscr{H}_X(U(L), \mathbf{t}) = \mathscr{E}(\mathscr{H}_X(L, \mathbf{t}))$.*

Доказательство основного результата основано на следующей точной формуле производящей функции для свободной полинильпотентной супералгебры Ли (см. [25]). Один частный случай этой формулы, а именно, формула для свободных метабелевых супералгебр Ли $F(\mathbf{A}^2, m, k)$ была найдена в [2] (см. также [14]).

Теорема 3.1 (см. [25]). *Пусть $L = F(\mathbf{N}_{s_q}\cdots\mathbf{N}_{s_2}\mathbf{N}_{s_1}, X)$ — свободная полинильпотентная супералгебра Ли, порожденная не более чем счетным порождающим множеством $X = \{x_i \mid i\in I\}$, где $I = I_+ \cup I_-$ и $X_+ = \{x_i \mid i\in I_+\}$, $X_- = \{x_i \mid i\in I_-\}$ — соответственно четные и нечетные порождающие. Определим функции $g_i(\mathbf{t})$, $f_i(\mathbf{t}) \in \mathbb{Q}[[\mathbf{t}]]$, $i = 0, \ldots, q$ следующим образом*: $g_0(\mathbf{t}) = 0$, $f_0(\mathbf{t}) = \sum\limits_{i\in I} t_i$ *и*

$$\begin{aligned} g_i(\mathbf{t}) &= g_{i-1}(\mathbf{t}) + \sum_{m=1}^{s_i}\frac{1}{m}\sum_{a|m}\mu(a)\left(f_{i-1}^{[a]}(\mathbf{t})\right)^{m/a}, && 1\leqslant i\leqslant q;\\ f_i(\mathbf{t}) &= 1 + \left(\sum_{i\in I} t_i - 1\right)\cdot\mathscr{E}(g_i(\mathbf{t})), && 1\leqslant i\leqslant q.\end{aligned}$$

Тогда $\mathscr{H}_X(L, \mathbf{t}) = g_q(\mathbf{t})$.

Далее предполагаем, что порождающее множество конечно. Пусть $I = I_+\cup I_-$, $I_+ = \{1, \ldots, m\}$, $I_- = \{m+1, m+2, \ldots, m+k\}$, $1 < m+k < \infty$. Имеем порождающее множество $X = X_+\cup X_-$, где $X_+ = \{x_1, \ldots, x_m\}$ и $X_- = \{x_{m+1}, \ldots, x_{m+k}\}$. Пусть $W \subset A$ — полиоднородное подпространство; тогда можно рассмотреть градуировки полистепенью W_α, степенью W_n, и «суперстепенью» W_{ij}, где последнее пространство состоит из элементов степени i относительно X_+ и степени j относительно X_-. Получаем следующие различные ряды Гильберта—Пуанкаре:

$$\mathscr{H}_X(W, \mathbf{t}) = \mathscr{H}(W, t_1, \ldots, t_{m+k}) = \sum_{\alpha\in\mathbb{N}_0^{m+k}} \dim W_\alpha\, t_1^{\alpha_1}\cdots t_{m+k}^{\alpha_{m+k}},$$

$$\mathscr{H}_X(W, x, y) = \sum_{i,j=0}^{\infty}\dim W_{ij}\, x^i y^j, \quad \mathscr{H}_X(W, t) = \sum_{n=0}^{\infty}\dim W_n\, t^n = \mathscr{H}(W, x, y)\Big|_{x=y=t}.$$

В [9] использовались переменные t_+, t_-, здесь, чтобы упростить формулы, мы будем использовать символы x, y и надеемся, что они не будут перепутаны с элементами порождающего множества X.

Применив теорему 3.1, полагая $t_i = x$ для $i \in I_+$ и $t_i = y$ для $i \in I_-$ в формуле $\mathscr{H}(L, \mathbf{t})$, получим $\mathscr{H}(L, x, y)$. Введенные выше операторы в этом случае выглядят следующим образом:

$$\phi^{[-]}(x,y) = \phi(x,-y), \quad \phi^{[m]}(x,y) = \phi(x^m, (-1)^{m+1}y^m),$$

$$\mathscr{E}(\phi(x,y)) = \exp\Big(\sum_{m=1}^{\infty} \frac{1}{m}\phi\big(x^m, (-1)^{m+1}y^m\big)\Big),$$

$$\mathscr{E}\Big(\sum_{i,j\geqslant 0;\ i+j>0} b_{ij}x^iy^j\Big) = \prod_{i,j}\big(1-(-1)^j x^i y^j\big)^{(-1)^{j+1}b_{ij}}.$$

Эти и другие формулы использовались ранее для получения формул размерностей компонент свободной супералгебры Ли и для изучения инвариантов конечных групп, действующих на свободных супералгебрах Ли [8, 9, 24, 29].

Получив точную формулу для ряда $\mathscr{H}(L, x, y)$, мы рассматриваем $\mathscr{H}(L, t) = \mathscr{H}(L, x, y)|_{x=t, y=t}$. Дальнейшие рассуждения аналогичны случаю алгебр Ли [23], при этом используются различные асимптотические методы [10, 26].

Для доказательства основного результата также изучается рост универсальных обертывающих алгебр супералгебр Ли [17]. Более того, построены некоторые специальные базисы для свободных супералгебр Ли [17].

СПИСОК ЛИТЕРАТУРЫ

1. *Бахтурин Ю. А.* Тождества в алгебрах Ли. — М.: Наука, 1985.
2. *Бахтурин Ю. А., Дренски В. С.* Тождества свободных разрешимых цветных супералгебр Ли// Алгебра и логика. — 1987. — *26*, № 4. — С. 403–418.
3. *Бокуть Л. А.* База свободных полинильпотентных алгебр Ли// Алгебра и логика. — 1963. — *2*, № 4. — С. 13–20.
4. *Гульден Я., Джексон Д.* Перечислительная комбинаторика. — М.: Наука, 1990.
5. *Егорычев Г. П.* Интегральное представление и вычисление комбинаторных сумм. — М.: Наука, 1977.
6. Коуровская тетрадь. Нерешенные проблемы теории групп. — Новосибирск: Наука, 1967.
7. *Петроградский В. М.* О некоторых типах промежуточного роста в алгебрах Ли// Усп. мат. наук. — 1993. — *48*, № 5. — С. 181–182.
8. *Петроградский В. М.* Об инвариантах действия конечной группы на свободной алгебре Ли// Сиб. мат. ж. — 2000. — *41*, № 4. — С. 915–925.
9. *Петроградский В. М.* Характеры и инварианты свободных супералгебр Ли// Алгебра и анализ. — 2001. — *13*, № 1. — С. 158–181.
10. *Постников А. Г.* Тауберова теория и ее приложения// Тр. Мат. ин-та им. В. А. Стеклова АН СССР. — 1979. — *144*.
11. *Стенли Р.* Перечислительная комбинаторика. — М.: Мир, 1990.
12. *Уфнаровский В. А.* Комбинаторные и асимптотические методы в алгебре// Итоги науки и техн. Совр. пробл. мат. Фундам. напр. — М.: ВИНИТИ, 1989. — *57*. — С. 5–177.
13. *Шмелькин А. Л.* Свободные полинильпотентные группы// Изв. АН СССР. Сер. мат. — 1964. — *28*, № 1. — С. 91–122.
14. *Bakhturin Yu. A., Mikhalev A. A., Petrogradsky V. M., Zaitsev M. V.* Infinite-dimensional Lie superalgebras/ de Gruyter Exp. Math. — Berlin: de Gruyter, 1992. — *7*.
15. *Borho W. and Kraft H.* Über die Gelfand–Kirillov Dimension// Math. Ann. — 1976. — *220*, № 1. — С. 1–24.
16. *Gelfand I. M., Kirillov A. A.* Sur les corps lies aux algèbres enveloppantes des algèbres de Lie// Inst. Hautes Études Sci. Publ. Math. — 1966. — *31*. — С. 509–523.
17. *Klementyev S. G. and Petrogradsky V. M.* Growth of solvable Lie superalgebras/ Manuscript.
18. *Krause G. R., Lenagan T. H.* Growth of algebras and Gelfand–Kirillov dimension/ Grad. Stud. Math. — Providence, Rhode Island: Amer. Math. Soc., 2000. — *22*.
19. *Lichtman A. I.* Growth in enveloping algebras// Israel J. Math. — 1984. — *47*, № 4. — С. 297–304.
20. *McConnell J. C., Robson J. C.* Noncommutative Noetherian rings. — Providence, Rhode Island: Amer. Math. Soc., 2001.

21. *Mikhalev A. A., Zolotykh A. A.* Combinatorial aspects of Lie superalgebras. — Boca Raton: CRC Press, 1995.
22. *Petrogradsky V. M.* Intermediate growth in Lie algebras and their enveloping algebras// J. Algebra. — 1996. — *179*. — С. 459–482.
23. *Petrogradsky V. M.* Growth of finitely generated polynilpotent Lie algebras and groups, generalized partitions, and functions analytic in the unit circle// Int. J. Algebra Comput. — 1999. — *9*, № 2. — С. 179–212.
24. *Petrogradsky V. M.* On Witt's formula and invariants for free Lie superalgebras// in: «Formal power series and algebraic combinatorics». — Springer-Verlag, 2000. — С. 543–551.
25. *Petrogradsky V. M.* On generating functions for subalgebras of free Lie superalgebras// Discr. Math. — 2002. — *246*, №№ 1–3. — С. 269–284.
26. *Ramanujan S.* Collected papers. — New York: Chelsea, 1962.
27. *Reutenauer C.* Free Lie algebras. — Oxford: Clarendon Press, 1993.
28. *Scheunert M.* The theory of Lie superalgebras. An introduction/ Lect. Notes Math. — Springer-Verlag, 1979. — *716*.
29. *Seok-Jin K.* Graded Lie superalgebras and the superdimension formula// J. Algebra. — 1998. — *204*, № 2. — С. 597–655.
30. *Stanley R. P.* Enumerative combinatorics. Vol. 2. — Cambridge Univ. Press, 1999.

С. Г. Клементьев
Ульяновский государственный университет
E-mail: klementyev@hotbox.ru

В. М. Петроградский
Ульяновский государственный университет
E-mail: petrogra@math.Uni-Duesseldorf.de; petrogradsky@hotbox.ru

Современная математика и ее приложения. Том 14 (2004). С. 48–70

УДК 512.62

РАЗНОСТНЫЕ РАЗМЕРНОСТНЫЕ МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

© 2004 г. **А. Б. ЛЕВИН**

Аннотация. Пусть K — разностное поле с базисным множеством мономорфизмов σ и пусть зафиксировано разбиение множества σ на p непересекающихся подмножеств. Пусть $\mathscr{D}$ — кольцо разностных операторов над K, рассматриваемое как фильтрованное кольцо с естественной p-мерной фильтрацией. Мы вводим специальный вид редукции в конечно порожденном свободном $\mathscr{D}$-модуле и развиваем соответствующую технику характеристических множеств, которая позволяет доказать, что сопоставляемая конечно порожденному разностному K-модулю функция Гильберта от p переменных полиномиальна. Мы также приводим идею метода вычисления такой функции и получаем обобщение принадлежащей автору теоремы о разностном размерностном многочлене. В заключение мы развиваем аналогичную технику характеристических множеств для кольца разностных многочленов и доказываем теорему о разностных размерностных многочленах, ассоциированных с конечно порожденными расширениями разностных полей.

СОДЕРЖАНИЕ

1. Введение

Эта работа посвящается Виктору Николаевичу Латышеву, который внес значительный вклад в современную теорию стандартных базисов и дал превосходное изложение этой теории в своих работах [3, 4, 15, 16]. В данной статье мы объединяем идеи метода стандартных базисов с теорией характеристических множеств Ритта—Колчина, чтобы доказать существование и в общих чертах изложить метод вычисления размерностных многочленов от нескольких переменных, связанных с конечно порожденными разностными векторными пространствами или расширениями разностных полей. Мы рассматриваем разбиение базисного множества сдвигов разностного поля K на p непересекающихся подмножеств ($p \geqslant 1$) и определяем редукцию в свободном разностном векторном пространстве над K, которая использует p упорядочений, связанных с разбиением. Редукции такого вида позволяют нам разработать соответствующую теорию характеристических множеств, которая приводит к теоремам о размерностных многочленах от нескольких переменных, ассоциированных с фильтрованными разностными модулями, и расширениям разностных полей. Мы излагаем идею метода вычисления таких многочленов и показываем, что они несут существенно больше разностных бирациональных инвариантов, чем стандартные размерностные многочлены от одной переменной.

ISSN 1512–1712

2. Предварительные сведения

В этом разделе мы излагаем некоторые основные понятия и результаты, которые используются в остальной части работы. Всюду далее $\mathbb{N}$, $\mathbb{Z}$ и $\mathbb{Q}$ обозначают множества неотрицательных целых чисел, целых чисел и рациональных чисел соответственно. Как обычно, $\mathbb{Q}[t]$ обозначает кольцо многочленов от одной переменной t с рациональными коэффициентами. Под кольцом мы всегда понимаем ассоциативное кольцо с единицей. Любой гомоморфизм колец унитарен (переводит единицу в единицу), любое подкольцо содержит единицу всего кольца. Если не оговорено противное, под модулем над кольцом R мы всегда понимаем унитарный левый R-модуль.

2.1. Разностные кольца и поля. *Разностное кольцо* — это коммутативное кольцо R с конечным множеством $\sigma = \{\alpha_1, \dots, \alpha_n\}$ попарно коммутирующих инъективных эндоморфизмов кольца R. Множество σ называется *базисным множеством* разностного кольца R, а эндоморфизмы $\alpha_1, \dots, \alpha_n$ — *базисными эндоморфизмами* или *трансляциями*. Разностное кольцо с базисным множеством σ также называется *σ-кольцом*. Если $\alpha_1, \dots, \alpha_n$ — автоморфизмы R, то будем говорить, что R — *инверсное разностное кольцо* с базисным множеством σ. Если разностное (σ-) кольцо является полем, то его называют разностным (σ-) полем.

Пусть R — разностное кольцо с базисным множеством σ, а R_0 — подкольцо в R, для которого $\alpha(R_0) \subseteq R_0$ для любого $\alpha \in \sigma$. Тогда R_0 называется *разностным* (или σ-) *подкольцом* в R, а кольцо R называется *разностным* (или σ-) *надкольцом* R_0. В этом случае ограничение эндоморфизма α_i на R_0 обозначается тем же символом α_i. Если R — разностное (σ-) поле и R_0 — подполе в R, для которого $\alpha(a) \in R_0$ для всех $a \in R_0, \alpha \in \sigma$, то R_0 называют разностным (или σ-) подполем в R; R, в свою очередь, называется разностным (или σ-) расширением или σ-надполем R_0. В этом случае мы можем также сказать, что у нас есть расширение σ-полей R/R_0.

Если R — разностное кольцо с базисным множеством σ, а J — идеал кольца R, для которого $\alpha(J) \subseteq J$ для всех $\alpha \in \sigma$, то J называется *разностным* (или σ-) идеалом R. Если простой (максимальный) идеал P в R замкнут относительно σ (т.е. $\alpha(P) \subseteq P$ для любого $\alpha \in \sigma$), то он называется *простым* (соответственно, *максимальным*) *разностным* (или σ-) *идеалом* R.

σ-Идеал J σ-кольца R называется *рефлексивным*, если для любого $\alpha \in \sigma$ включение $\alpha(a) \in J$ ($a \in R$) влечет $a \in J$.

Если R — разностное кольцо с базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_n\}$, то T_σ будет обозначать свободную коммутативную полугруппу с единицей, порожденную $\alpha_1, \dots, \alpha_n$. Элементы T_σ будут мультипликативно записываться в виде $\alpha_1^{k_1} \dots \alpha_n^{k_n}$ ($k_1, \dots, k_n \in \mathbb{N}$) и рассматриваться в качестве эндоморфизмов R. Для любого $a \in R$ и любого $\tau \in T_\sigma$ элемент $\tau(a)$ называется *трансформой* элемента a.

Пусть R — разностное кольцо с базисным множеством σ и $S \subseteq R$. Тогда пересечение всех σ-идеалов R, содержащих S, обозначается $[S]$. Ясно, что $[S]$ — наименьший σ-идеал в R, содержащий S; как идеал он порождается множеством

$$T_\sigma S = \{\tau(a) \mid \tau \in T_\sigma,\ a \in S\}.$$

Если $J = [S]$, то говорят, что σ-идеал J порождается множеством S, которое называется *множеством σ-порождающих* J. Если S конечно, $S = \{a_1, \dots, a_k\}$, то будем записывать это в виде $J = [a_1, \dots, a_k]$ и говорить, что J — конечно порожденный σ-идеал σ-кольца R. (В этом случае элементы $a_1, \dots, a_k$ называются σ-порождающими J.)

Пусть R — разностное кольцо с базисным множеством σ, R_0 — σ-подкольцо в R и $B \subseteq R$. Пересечение всех σ-подколец R, содержащих R_0 и B, называется *σ-подкольцом R, порожденным множеством B над R_0*, и обозначается $R_0\{B\}$. (Как кольцо $R_0\{B\}$ совпадает с кольцом $R_0[\{\tau(b) \mid b \in B, \tau \in T_\sigma\}]$, полученным присоединением множества $\{\tau(b) \mid b \in B, \tau \in T_\sigma\}$ к кольцу R_0). Множество B называют множеством *σ-порождающих* σ-кольца $R_0\{B\}$ над R_0. Если

это множество конечно, $B = \{b_1, \dots, b_k\}$, то будем говорить, что $R' = R_0\{B\}$ — конечно порожденное разностное (или σ-) расширение (или надкольцо) кольца R_0 и записывать это в виде $R' = R_0\{b_1, \dots, b_k\}$.

Если R — σ-поле, R_0 — σ-подполе в R и $B \subseteq R$, то пересечение всех σ-подполей R, содержащих R_0 и B, обозначается $R_0\langle B\rangle$ (или $R_0\langle b_1, \dots, b_k\rangle$, если $B = \{b_1, \dots, b_k\}$ — конечное множество). Это наименьшее σ-подполе в R, содержащее R_0 и B; оно совпадает с полем $R_0(\{\tau(b) \mid b \in B, \tau \in T_\sigma\})$. Множество B называется множеством *σ-порождающих* σ-поля $R_0\langle B\rangle$ над R_0.

В дальнейшем мы будем рассматривать два или более разностных кольца $R_1, \dots, R_p$ с одним и тем же базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_n\}$. Говоря формально, это означает, что для каждого $i = 1, \dots, p$ имеется фиксированное отображение ν_i из множества σ в множество инъективных эндоморфизмов кольца R_i, для которого любые два эндоморфизма $\nu_i(\alpha_j)$ и $\nu_i(\alpha_k)$ кольца R_i коммутируют ($1 \leqslant j, k \leqslant n$). Мы отождествим элементы α_j с их образами $\nu_i(\alpha_j)$ и будем говорить, что элементы множества σ действуют как попарно коммутирующие инъективные эндоморфизмы кольца R_i ($i = 1, \dots, p$).

Пусть R_1 и R_2 — разностные кольца с одним и тем же базисным множеством σ. Гомоморфизм колец $\phi : R_1 \to R_2$ называется *разностным* (или σ-) *гомоморфизмом*, если $\phi(\alpha(a)) = \alpha(\phi(a))$ для любого $\alpha \in \sigma, a \in R_1$. Если σ-гомоморфизм является изоморфизмом (эндоморфизмом, автоморфизмом и т. д.), то он называется разностным (или σ-) изоморфизмом (соответственно, разностным (или σ-) эндоморфизмом, разностным (или σ-) автоморфизмом и т. д.). Если R_1 и R_2 — два σ-надкольца одного и того же σ-кольца R_0 и $\phi : R_1 \to R_2$ — такой σ-гомоморфизм, что $\phi(a) = a$ для любого $a \in R_0$, то будем говорить, что ϕ — разностный (или σ-) гомоморфизм над R_0 или что ϕ оставляет кольцо R_0 на месте. Легко видеть, что ядро любого σ-гомоморфизма σ-колец $\phi : R \to R'$ является рефлексивным σ-идеалом в R. Наоборот, пусть g — сюръективный гомоморфизм σ-кольца R на кольцо S, для которого $\operatorname{Ker} g$ — рефлексивный разностный идеал в R. Тогда на S имеется единственная структура σ-кольца, в которой g является σ-гомоморфизмом. В частности, если I — рефлексивный σ-идеал σ-кольца R, то факторкольцо R/I обладает единственной структурой σ-кольца, в которой каноническая сюръекция $R \to R/I$ является σ-гомоморфизмом. В этом случае R/I называется *разностным* (или σ-) *факторкольцом* R по I.

Если разностное кольцо R с базисным множеством σ является областью целостности, то его поле частных $Q(R)$ можно естественным образом считать σ-надкольцом R. (Мы отождествляем элемент $a \in R$ с его каноническим образом $\frac{a}{1}$ в $Q(R)$.) В этом случае $Q(R)$ называется *разностным* (или σ-) *полем частных* R. Ясно, что если σ-кольцо R инверсно, то его σ-поле частных $Q(R)$ также инверсно. Далее, если σ-поле K содержит целостное кольцо R в качестве σ-подкольца, то K содержит его σ-поле частных $Q(R)$.

2.2. Разностные многочлены. Пусть R — разностное кольцо с базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_n\}$, T_σ — свободная коммутативная полугруппа, порожденная σ, а $U = \{u_\lambda \mid \lambda \in \Lambda\}$ — семейство элементов из какого-либо σ-надкольца R. Мы будем говорить, что семейство U *разностно* (или *σ-алгебраически) зависимо* над R, если семейство

$$T_\sigma(U) = \{\tau(u_\lambda) \mid \tau \in T_\sigma,\ \lambda \in \Lambda\}$$

алгебраически зависимо над R (т.е. существуют элементы $v_1, \dots, v_k \in T_\sigma(U)$ и ненулевой многочлен $f(X_1, \dots, X_k)$ с коэффициентами из R, для которого $f(v_1, \dots, v_k) = 0$). В противном случае семейство U называют *разностно* (или *σ-алгебраически) независимым* над R или семейством *разностных* (или σ-) *переменных* над R. В последнем случае σ-кольцо $R\{(u_\lambda)_{\lambda\in\Lambda}\}_\sigma$ называется *алгеброй разностных* (или σ-) *многочленов* от разностных (или σ-) переменных $\{(u_\lambda)_{\lambda\in\Lambda}\}$ над R. Если семейство, состоящее из одного элемента u, σ-алгебраически зависимо над R, то элемент u называется *разностно алгебраическим* (или *σ-алгебраическим*) над σ-кольцом R. Если множество $\{\tau(u) \mid \tau \in T\}$ алгебраически независимо над R, то мы будем говорить, что u *разностно* (или σ-) *трансцендентен* над кольцом R.

Пусть R — σ-поле, L — σ-надполе R и $S \subseteq L$. Мы говорим, что *множество S σ-алгебраично над R*, если каждый элемент $a \in S$ σ-алгебраичен над R. Если каждый элемент L σ-алгебраичен над R, мы говорим, что L — *σ-алгебраическое расширение* σ-поля R.

Предложение 2.1 (см. [9, Chap. 2, Theorem I], [14, Proposition 3.3.7]). *Пусть R — разностное кольцо с базисным множеством σ, а I — произвольное множество. Тогда существует алгебра σ-многочленов над R от семейства σ-переменных, индексированного множеством I. Если S и S' — две такие алгебры, то существует σ-изоморфизм $S \to S'$, оставляющий на месте кольцо R. Если R — область целостности, то любая алгебра σ-многочленов над R является областью целостности.*

Алгебру σ-многочленов из предложения 2.1 можно построить следующим образом. Пусть $T = T_\sigma$ и S — R-алгебра многочленов от переменных $\{y_{i,\tau}\}_{i\in I,\tau\in T}$ с индексами из множества $I \times T$. Для любого $f \in S$ и $\alpha \in \sigma$ пусть $\alpha(f)$ обозначает многочлен из S, полученный заменой каждой переменной $y_{i,\tau}$, входящей в f, на $y_{i,\alpha\tau}$ и любого коэффициента $a \in R$ на $\alpha(a)$. Мы получаем инъективный эндоморфизм $S \to S$, который продолжает исходный эндоморфизм α кольца R на кольцо S (это продолжение обозначается той же буквой α). Полагая $y_i = y_{i,1}$ (где 1 обозначает единицу полугруппы T), мы получаем σ-алгебраически независимое над R множество $\{y_i \mid i \in I\}$, для которого $S = R\{(y_i)_{i\in I}\}$. Таким образом, S — алгебра σ-многочленов над R от семейства σ-переменных $\{y_i \mid i \in I\}$.

2.3. Кольцо разностных операторов. Разностные модули. Пусть R — разностное кольцо с базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_n\}$, а T — свободная коммутативная полугруппа, порожденная элементами $\alpha_1, \dots, \alpha_n$. Если $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ $(k_1, \dots, k_n \in \mathbb{N})$, то число $\operatorname{ord}\tau = \sum\limits_{\nu=1}^{n} k_\nu$ называется *порядком* τ. Далее, для любого $r \in \mathbb{N}$ множество $\{\tau \in T \mid \operatorname{ord}\tau \leqslant r\}$ обозначается символом $T(r)$.

Определение 2.2. Выражение вида $\sum\limits_{\tau\in T} a_\tau\tau$, где $a_\tau \in R$ для любого $\tau \in T$ и только конечное число элементов a_τ отличны от 0, называется разностным (или σ-) оператором над разностным кольцом R. Два σ-оператора $\sum\limits_{\tau\in T} a_\tau\tau$ и $\sum\limits_{\tau\in T} b_\tau\tau$ считаются равными, если и только если $a_\tau = b_\tau$ для любого $\tau \in T$.

Пусть $\mathscr{D}$ — множество всех σ-операторов над σ-кольцом R. Это множество можно снабдить структурой кольца, полагая

$$\sum_{\tau\in T} a_\tau\tau + \sum_{\tau\in T} b_\tau\tau = \sum_{\tau\in T} (a_\tau + b_\tau)\tau, \quad a\sum_{\tau\in T} a_\tau\tau = \sum_{\tau\in T} (aa_\tau)\tau,$$
$$\left(\sum_{\tau\in T} a_\tau\tau\right)\tau_1 = \sum_{\tau\in T} a_\tau(\tau\tau_1), \quad \tau_1 a = \tau_1(a)\tau_1$$

для любых $\sum\limits_{\tau\in T} a_\tau\tau$, $\sum\limits_{\tau\in T} b_\tau\tau \in \mathscr{D}$, $a \in R$, $\tau_1 \in T$ и продолжая умножение по дистрибутивности. Получаемое таким образом кольцо называется *кольцом разностных* (или σ-) *операторов над R*.

Порядок σ-оператора $A = \sum\limits_{\tau\in T} a_\tau\tau \in \mathscr{D}$ определяется как число $\operatorname{ord} A = \max\{\operatorname{ord}\tau \mid a_\tau \neq 0\}$. Если положить $\mathscr{D}_r = \{A \in \mathscr{D} \mid \operatorname{ord} A \leqslant r\}$ для любого $r \in \mathbb{N}$ и $\mathscr{D}_r = 0$ для любого $r \in \mathbb{Z}$, $r < 0$, то кольцо $\mathscr{D}$ можно рассматривать как фильтрованное кольцо с возрастающей фильтрацией $(\mathscr{D}_r)_{r\in\mathbb{Z}}$. Ниже, рассматривая $\mathscr{D}$ как фильтрованное кольцо, мы всегда имеем в виду эту фильтрацию.

Определение 2.3. Пусть R — разностное кольцо с базисным множеством σ, а $\mathscr{D}$ — кольцо σ-операторов над R. Тогда левый $\mathscr{D}$-модуль называется разностным R-модулем или σ-R-модулем. Другими словами, R-модуль M — это разностный (или σ-) R-модуль, если элементы σ действуют

на M таким образом, что $\alpha(x+y)=\alpha(x)+\alpha(y)$, $\alpha(\beta x)=\beta(\alpha x)$ и $\alpha(ax)=\alpha(a)\alpha(x)$ для любых $x,y\in M;\alpha,\beta\in\sigma;\ a\in R$.

Если R — разностное (σ-) поле, то σ-R-модуль M также называют разностным векторным пространством над R или векторным σ-R-пространством.

Мы говорим, что разностный R-модуль M конечно порожден, если он конечно порожден как левый $\mathscr{D}$-модуль. Под фильтрованным σ-R-модулем мы всегда понимаем левый $\mathscr{D}$-модуль, снабженный исчерпывающей и отделимой фильтрацией. Таким образом, фильтрация σ-R-модуля M — это возрастающая цепочка $(M_r)_{r\in\mathbb{Z}}$ R-подмодулей M, для которой $\mathscr{D}_r M_s\subseteq M_{r+s}$ для всех $r,s\in\mathbb{Z}$, $M_r=0$ для всех достаточно малых $r\in\mathbb{Z}$ и $\bigcup\limits_{r\in\mathbb{Z}} M_r=M$.

Фильтрация $(M_r)_{r\in\mathbb{Z}}$ σ-R-модуля M называется *отличной*, если все R-модули M_r ($r\in\mathbb{Z}$) конечно порождены и существует $r_0\in\mathbb{Z}$, для которого $M_r=\mathscr{D}_{r-r_0}M_{r_0}$ для любого $r\in\mathbb{Z}$, $r\geqslant r_0$.

Следующий результат был получен в [5] (см. также [14, Theorem 6.2.5]).

Теорема 2.4. *Пусть R — артиново разностное кольцо с базисным множеством $\sigma=\{\alpha_1,\dots,\alpha_n\}$, $\mathscr{D}$ — кольцо σ-операторов над R, а $(M_r)_{r\in\mathbb{Z}}$ — отличная фильтрация σ-R-модуля M. Тогда существует многочлен $\psi(t)\in\mathbb{Q}[t]$ со следующими свойствами.*

(i) *$\psi(r)=l_R(M_r)$ для всех достаточно больших $r\in\mathbb{Z}$ (т.е. существует такое $r_0\in\mathbb{Z}$, что последнее равенство выполнено для всех целых $r\geqslant r_0$).*

(ii) *$\deg\psi(t)\leqslant n$, и многочлен $\psi(t)$ можно записать в виде*

$$\psi(t)=\sum_{i=0}^{n} c_i\binom{t+i}{i},$$

где $c_0,c_1,\dots,c_n\in\mathbb{Z}$.[1]

(iii) *Если R — разностное поле, то целые числа $d=\deg\psi(t)$, c_n и c_d (если $d<n$) не зависят от выбора отличной фильтрации на M. Кроме того, c_n равно максимальному числу элементов M, линейно независимых над $\mathscr{D}$.*

Многочлен $\psi(t)$, существование которого устанавливается в теореме 2.4, называется *разностным (σ-) размерностным многочленом* или *характеристическим многочленом* σ-R-модуля M, ассоциированным с отличной фильтрацией $(M_r)_{r\in\mathbb{Z}}$. Если R — разностное поле, то целые числа d, c_n и c_d называются *разностным типом*, *разностной размерностью* и *типовой разностной размерностью* M соответственно.

Теорема 2.4 является разностной версией теоремы о дифференциальном размерностном многочлене, доказанной в [10]. Ряд результатов, касающихся дифференциальных и разностных размерностных многочленов и методов их вычисления, представлен в [2, 6–8, 17, 18] и в [14, Chaps. 5–9].

2.4. Разбиения базисного множества и многомерные фильтрации разностных модулей. Пусть R — дифференциальное поле с базисным множеством $\sigma=\{\alpha_1,\dots,\alpha_n\}$, T — коммутативная полугруппа всевозможных произведений $\alpha_1^{k_1}\dots\alpha_n^{k_n}$ ($k_1,\dots,k_n\in\mathbb{N}$) и $\mathscr{D}$ — кольцо σ-операторов на R. Пусть зафиксировано некоторое разбиение множества σ на непересекающиеся подмножества:

$$\sigma=\sigma_1\cup\dots\cup\sigma_p, \tag{1}$$

где $p\in\mathbb{N}$ и $\sigma_1=\{\alpha_1,\dots,\alpha_{n_1}\}$, $\sigma_2=\{\alpha_{n_1+1},\dots,\alpha_{n_1+n_2}\}$, …, $\sigma_p=\{\alpha_{n_1+\dots+n_{p-1}+1},\dots,\alpha_n\}$ ($n_i\geqslant 1$ при $i=1,\dots,p$; $n_1+\dots+n_p=n$).

[1] Как обычно, $\binom{t+i}{i}$ обозначает многочлен $\dfrac{(t+i)(t+i-1)\dots(t+1)}{i!}\in\mathbb{Q}[t]$, принимающий целые значения для всех достаточно больших целых t.

Если $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ $(k_1, \dots, k_n \in \mathbb{N})$, то числа

$$\operatorname{ord}_i \tau = \sum_{\nu=n_1+\dots+n_{i-1}+1}^{n_1+\dots+n_i} k_\nu, \quad 1 \leqslant i \leqslant p,$$

называются *порядками* τ по отношению к σ_i (мы предполагаем, что $n_0 = 0$, так что индексы в сумме для $\operatorname{ord}_1 \tau$ меняются от 1 до n_1). Как и прежде, порядок элемента τ определяется формулой

$$\operatorname{ord} \tau = \sum_{\nu=1}^{n} k_i = \sum_{i=1}^{p} \operatorname{ord}_i \tau.$$

Ниже мы будем рассматривать порядки $<_1, \dots, <_p$ на множестве T, определяемые следующим образом:

$$\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} <_i \tau' = \alpha_1^{l_1} \dots \alpha_n^{l_n}$$

тогда и только тогда, когда вектор

$$(\operatorname{ord}_i \tau, \operatorname{ord} \tau, \operatorname{ord}_1 \tau, \dots, \operatorname{ord}_{i-1} \tau, \operatorname{ord}_{i+1} \tau, \dots, \operatorname{ord}_p \tau,$$
$$k_{n_1+\dots+n_{i-1}+1}, \dots, k_{n_1+\dots+n_i}, k_1, \dots, k_{n_1+\dots+n_{i-1}}, k_{n_1+\dots+n_i+1}, \dots, k_n)$$

меньше вектора

$$(\operatorname{ord}_i \tau', \operatorname{ord} \tau', \operatorname{ord}_1 \tau', \dots, \operatorname{ord}_{i-1} \tau', \operatorname{ord}_{i+1} \tau', \dots, \operatorname{ord}_p \tau',$$
$$l_{n_1+\dots+n_{i-1}+1}, \dots, l_{n_1+\dots+n_i}, l_1, \dots, l_{n_1+\dots+n_{i-1}}, l_{n_1+\dots+n_i+1}, \dots, l_n)$$

относительно лексикографического упорядочения на $\mathbb{N}^{n+p+1}$. Легко видеть, что множество T вполне упорядочено относительно каждого из порядков $<_1, \dots, <_p$.

Если $r_1, \dots, r_p$ — неотрицательные целые числа, то $T(r_1, \dots, r_p)$ будет обозначать множество всех элементов $\tau \in T$ таких, что $\operatorname{ord}_i \tau \leqslant r_i$ $(i = 1, \dots, p)$. Векторное K-подпространство в $\mathscr{D}$, порожденное множеством $T(r_1, \dots, r_p)$, будет обозначаться через $\mathscr{D}_{r_1,\dots,r_p}$.

Полагая $\mathscr{D}_{r_1,\dots,r_p} = 0$ для всех $(r_1, \dots, r_p) \in \mathbb{Z}^p \setminus \mathbb{N}^p$, получаем семейство

$$\{\mathscr{D}_{r_1,\dots,r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$$

K-подпространств в $\mathscr{D}$, которое называется *стандартной p-мерной фильтрацией* кольца $\mathscr{D}$. Легко видеть, что $\mathscr{D}_{r_1,\dots,r_p} \subseteq \mathscr{D}_{s_1,\dots,s_p}$, если $(r_1, \dots, r_p) \leqslant_P (s_1, \dots, s_p)$, где $\leqslant_P$ обозначает порядок на прямом произведении $\mathbb{Z}^p$ (т.е. частичный порядок на $\mathbb{Z}^p$ такой, что $(a_1, \dots, a_p) \leqslant_P (b_1, \dots, b_p)$ тогда и только тогда, когда $a_i \leqslant b_i$ для $i = 1, \dots, p$). Более того, $\mathscr{D}_{i_1,\dots,i_p} \mathscr{D}_{r_1,\dots,r_p} = \mathscr{D}_{r_1+i_1,\dots,r_p+i_p}$ для всех $(r_1, \dots, r_p), (i_1, \dots, i_p) \in \mathbb{N}^p$.

Определение 2.5. Пусть M — векторное σ-K-пространство (т.е. левый $\mathscr{D}$-модуль). Семейство

$$\{M_{r_1,\dots,r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$$

называется p-мерной фильтрацией M, если выполнены следующие четыре условия:

(i) для каждого набора из p элементов $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbb{Z}^p$ такого, что $(r_1, \dots, r_p) \leqslant_P (s_1, \dots, s_p)$, имеем:

$$M_{r_1,\dots,r_p} \subseteq M_{s_1,\dots,s_p};$$

(ii) $\bigcup_{(r_1,\dots,r_p)\in\mathbb{Z}^p} M_{r_1,\dots,r_p} = M$;

(iii) существует набор из p элементов $(r_1^{(0)}, \dots, r_p^{(0)}) \in \mathbb{Z}^p$ такой, что $M_{r_1,\dots,r_p} = 0$, если $r_i < r_i^{(0)}$ по крайней мере для одного индекса i $(1 \leqslant i \leqslant p)$.

(iv) $\mathscr{D}_{r_1,\dots,r_p} M_{s_1,\dots,s_p} \subseteq M_{r_1+s_1,\dots,r_p+s_p}$ для каждого $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbb{Z}^p$.

Если каждое векторное K-пространство $M_{r_1,\dots,r_p}$ конечномерно и существует элемент $(h_1,\dots,h_p)\in\mathbb{Z}^p$ такой, что $\mathscr{D}_{r_1,\dots,r_p}M_{h_1,\dots,h_p}=M_{r_1+h_1,\dots,r_p+h_p}$ для любого $(r_1,\dots,r_p)\in\mathbb{N}^p$, то p-мерная фильтрация

$$\{M_{r_1,\dots,r_p}\mid (r_1,\dots,r_p)\in\mathbb{Z}^p\}$$

называется *отличной*.

Легко видеть, что если $z_1,\dots,z_k$ — конечная система образующих векторного σ-K-пространства M, то

$$\left\{\sum_{i=1}^{k}\mathscr{D}_{r_1,\dots,r_p}z_i\mid (r_1,\dots,r_p)\in\mathbb{Z}^p\right\}$$

— отличная p-мерная фильтрация M.

2.5. Целозначные многочлены. Многочлен $f(t_1,\dots,t_p)$ от p переменных $t_1,\dots,t_p$ $(p\geqslant 1)$ с рациональными коэффициентами называется *целозначным*, если $f(t_1,\dots,t_p)\in\mathbb{Z}$ для всех достаточно больших $t_1,\dots,t_p\in\mathbb{Z}$, т.е. найдется элемент $(s_1,\dots,s_p)\in\mathbb{Z}^p$ такой, что $f(r_1,\dots,r_p)\in\mathbb{Z}$ при любых $(r_1,\dots,r_p)\in\mathbb{Z}^p$ и $r_i\geqslant s_i$ для всех $i=1,\dots,p$.

Ясно, что каждый многочлен с целыми коэффициентами является целозначным. В качестве примера целозначного многочлена от p переменных с нецелыми коэффициентами можно взять многочлен $\prod\limits_{i=1}^{p}\binom{t_i}{m_i}$, где $m_1,\dots,m_p\in\mathbb{N}$.

Если f — целозначный многочлен от p переменных и $p>1$, то $\deg f$ и $\deg_{t_i} f$ $(1\leqslant i\leqslant p)$ будут обозначать полную степень f и степень f относительно переменной t_i соответственно. Следующая теорема, доказанная в [13], дает «каноническое» представление целозначного многочлена от нескольких переменных.

Теорема 2.6. *Пусть $f(t_1,\dots,t_p)$ — целозначный многочлен от $t_1,\dots,t_p$ и $\deg_{t_i} f=m_i$ $(m_1,\dots,m_p\in\mathbb{N})$. Тогда многочлен $f(t_1,\dots,t_p)$ может быть представлен формулой*

$$f(t_1,\dots t_p)=\sum_{i_1=0}^{m_1}\cdots\sum_{i_p=0}^{m_p}a_{i_1\dots i_p}\binom{t_1+i_1}{i_1}\dots\binom{t_p+i_p}{i_p}\tag{2}$$

с целыми коэффициентами $a_{i_1\dots i_p}$, однозначно определенными целозначным многочленом.

В дальнейшем (до конца этого раздела) мы будем иметь дело с подмножествами множества $\mathbb{N}^m$, где натуральное число m представлено в виде суммы p неотрицательных целых чисел $m_1,\dots,m_p$ $(p\in\mathbb{N},\ p\geqslant 1)$. Другими словами, мы предполагаем, что зафиксировано разбиение $(m_1,\dots,m_p)$ числа m.

Если $\mathscr{A}\subseteq\mathbb{N}^m$, то для любых $r_1,\dots,r_p\in\mathbb{N}$ обозначим через $\mathscr{A}(r_1,\dots,r_p)$ подмножество $\mathscr{A}$, состоящее из всех элементов $(a_1,\dots,a_m)$ таких, что

$$a_1+\dots+a_{m_1}\leqslant r_1,\quad a_{m_1+1}+\dots+a_{m_1+m_2}\leqslant r_2,\quad\dots,\quad a_{m_1+\dots+m_{p-1}+1}+\dots+a_m\leqslant r_p.$$

Более того, с множеством $\mathscr{A}$ мы будем ассоциировать множество $V_{\mathscr{A}}\subseteq\mathbb{N}$, состоящее из всех элементов $v=(v_1,\dots,v_m)\in\mathbb{N}$, которые не превосходят любого элемента $\mathscr{A}$ относительно порядка прямого произведения на $\mathbb{N}^m$. Очевидно, что элемент $v=(v_1,\dots,v_m)\in\mathbb{N}^m$ принадлежит $V_{\mathscr{A}}$ тогда и только тогда, когда для любого элемента $(a_1,\dots,a_m)\in\mathscr{A}$ существует $i\in\mathbb{N}$, $1\leqslant i\leqslant m$, такой, что $a_i>v_i$.

Две следующие теоремы, доказанные в [13], обобщают известный результат Колчина о целозначных многочленах от одной переменной для подмножеств $\mathbb{N}^m$ (см. [12, Chap. 0, Lemma 17]) и дают точную формулу для целозначных многочленов от p переменных, ассоциированных с конечным подмножеством $\mathbb{N}^m$.

Теорема 2.7. *Пусть $\mathscr{A}$ — подмножество $\mathbb{N}^m$, где $m = m_1 + \cdots + m_p$ для некоторых неотрицательных целых чисел $m_1, \ldots, m_p$ ($p \geqslant 1$). Тогда существует целозначный многочлен $\omega_{\mathscr{A}}(t_1, \ldots, t_p)$ со следующими свойствами*:

(i) $\omega_{\mathscr{A}}(r_1, \ldots, r_p) = \operatorname{Card} V_{\mathscr{A}}(r_1, \ldots, r_p)$ *для всех достаточно больших* $(r_1, \ldots, r_p) \in \mathbb{N}^p$ (*как обычно,* $\operatorname{Card} M$ *обозначает число элементов конечного множества* M).

(ii) *Полная степень многочлена* $\omega_{\mathscr{A}}$ *не превосходит* m *и* $\deg_{t_i} \omega_{\mathscr{A}} \leqslant m_i$ *для всех* $i = 1, \ldots, p$.

(iii) $\deg \omega_{\mathscr{A}} = m$ *тогда и только тогда, когда множество* $\mathscr{A}$ *пусто. В этом случае* $\omega_{\mathscr{A}}(t_1, \ldots, t_p) = \prod_{i=1}^{p} \binom{t_i + m_i}{m_i}$.

(iv) $\omega_{\mathscr{A}}$ *— нулевой многочлен тогда и только тогда, когда* $(0, \ldots, 0) \in A$.

Определение 2.8. Многочлен $\omega_{\mathscr{A}}(t_1, \ldots, t_p)$, существование которого утверждается в теореме 2.7, называется *размерностным многочленом* множества $\mathscr{A} \subseteq \mathbb{N}^m$, ассоциированным с разбиением $(m_1, \ldots, m_p)$ числа m. Если $p = 1$, то многочлен $\omega_{\mathscr{A}}$ называется многочленом Колчина множества $\mathscr{A}$.

Теорема 2.9. *Пусть $\mathscr{A} = \{a_1, \ldots, a_n\}$ — конечное подмножество $\mathbb{N}^m$, где m — натуральное число и $m = m_1 + \cdots + m_p$ для некоторых неотрицательных целых чисел $m_1, \ldots, m_p$, $p \geqslant 1$. Пусть $a_i = (a_{i1}, \ldots, a_{im})$, $1 \leqslant i \leqslant n$, и для каждого $l \in \mathbb{N}$, $0 \leqslant l \leqslant n$, пусть $\Gamma(l, n)$ обозначает множество всех l-элементных подмножеств множества $\mathbb{N}_n = \{1, \ldots, n\}$. Более того, для всех $\xi \in \Gamma(l, p)$ положим*

$$\bar{a}_{\xi h} = \max\{a_{ih} \mid i \in \xi\}, \quad 1 \leqslant h \leqslant m, \qquad b_{\xi j} = \sum_{h \in \sigma_j} \bar{a}_{\xi h}.$$

(*Если $\xi = \emptyset$, мы предполагаем, что $\bar{a}_{\xi h} = 0$ для $h = 1, \ldots, m$, так что $b_{\xi j} = 0$ для $j = 1, \ldots, p$.*) *Тогда*

$$\omega_{\mathscr{A}}(t_1, \ldots, t_p) = \sum_{l=0}^{n} (-1)^l \sum_{\xi \in \Gamma(l,n)} \prod_{j=1}^{p} \binom{t_j + m_j - b_{\xi j}}{m_j}. \tag{3}$$

Очевидно, что если $\mathscr{A}$ — некоторое подмножество $\mathbb{N}^m$ и $\mathscr{A}'$ — множество всех минимальных элементов множества $\mathscr{A}$ относительно порядка прямого произведения на $\mathbb{N}^m$, то множество $\mathscr{A}'$ конечно и $\omega_{\mathscr{A}}(t_1, \ldots, t_p) = \omega_{\mathscr{A}'}(t_1, \ldots, t_p)$. Таким образом, теорема 2.9 дает алгоритм, позволяющий найти целозначный многочлен, ассоциированный с любым подмножеством $\mathbb{N}^m$ (и с заданным представлением m в виде суммы p неотрицательных целых чисел): сначала нужно найти множество всех минимальных точек подмножества и затем применить теорему 2.9.

3. Редукция в свободном разностном векторном пространстве. Характеристические множества

Пусть K — разностное поле с базисным множеством $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, T — свободная коммутативная полугруппа, порожденная σ, и $\mathscr{D}$ — кольцо σ-операторов над K. Кроме того, мы предполагаем, что зафиксировано разбиение (1) множества σ.

Под *свободным векторным σ-K-пространством* мы понимаем векторное σ-K-пространство, являющееся свободным модулем над кольцом разностных операторов $\mathscr{D}$. Пусть E — конечно порожденный свободный левый $\mathscr{D}$-модуль со свободными образующими $e_1, \ldots, e_k$ (мы также говорим, что E — свободное векторное σ-K-пространство с этими свободными образующими). В дальнейшем элементы вида τe_ν ($\tau \in T, 1 \leqslant \nu \leqslant k$) будем называть *термами*, а элементы полугруппы T — *мономами*. Множество всех термов обозначаем через Te. Легко видеть, что это множество порождает E как векторное пространство над полем K.

Под порядком терма τe_ν относительно σ_i ($1 \leqslant i \leqslant p$) понимаем порядок монома τ по отношению к σ_i. Терм $u' = \tau' e_\mu$ называется *кратным* терма $u = \tau e_\nu$, если $\mu = \nu$ и τ' кратен τ в полугруппе

T. В этом случае мы пишем $u|u'$. (Очевидно, $u|u'$ тогда и только тогда, когда существует $\tau'' \in T$, такой что $u' = \tau'' u$.)

Будем рассматривать p порядков на множестве Te, соответствующих упорядочениям полугруппы T, рассмотренным в предыдущем разделе. Эти упорядочения обозначаются теми же символами $<_1, \dots, <_p$ и определяются следующим образом: если $\tau e_\mu, \tau' e_\mu \in Te$, то $\tau e_\mu <_i \tau' e_\nu$ тогда и только тогда, когда $\tau <_i \tau'$ в T или $\tau = \tau'$ и $\mu < \nu$.

Так как множество Te — базис векторного K-пространства E, то каждый элемент $f \in E$ имеет единственное представление вида

$$f = a_1 \tau_1 e_{i_1} + \dots + a_l \tau_l e_{i_l}, \tag{4}$$

где $\tau_i \in T$, $a_i \in K$, $a_i \neq 0$ $(1 \leqslant i \leqslant l)$ и $1 \leqslant i_1, \dots, i_l \leqslant k$.

Определение 3.1. Пусть f — элемент модуля E, записанный в виде (4), и пусть $\tau_\nu e_{i_\nu}$ $(1 \leqslant \nu \leqslant p)$ — наибольший терм в множестве $\{\tau_1 e_{i_1}, \dots, \tau_l e_{i_l}\}$ относительно порядка $<_j$ $(1 \leqslant j \leqslant p)$. Тогда терм $\tau_\nu e_{i_\nu}$ называется j-лидером элемента f и обозначается через $u_f^{(j)}$. (Конечно, возможно, что $u_f^{(j)} = u_f^{(j')}$ для некоторых различных чисел j и j'.)

В дальнейшем будем говорить, что элемент $f \in E$ содержит терм τe_ν, если этот терм участвует в представлении (4) с ненулевым коэффициентом. Коэффициент j-лидера элемента $f \in E$ будет обозначаться через $\mathrm{lc}_j(f)$ $(1 \leqslant j \leqslant p)$.

Определение 3.2. Пусть f и g — два элемента свободного $\mathscr{D}$-модуля E, рассмотренного выше. Элемент f называется редуцированным относительно g, если f не содержит никакого кратного $\tau u_g^{(1)}$ $(\tau \in T)$ 1-лидера $u_g^{(1)}$ такого, что $\mathrm{ord}_j(\tau u_g^{(j)}) \leqslant \mathrm{ord}_j u_f^{(j)}$ при $j = 2, \dots, p$. Элемент $h \in E$ называется редуцированным относительно множества $\Sigma \subseteq E$, если h редуцирован относительно каждого элемента этого множества Σ.

Определение 3.3. Подмножество Σ свободного $\mathscr{D}$-модуля E называется авторедуцированным, если каждый элемент Σ редуцирован относительно всех остальных элементов данного множества. Авторедуцированное множество Σ называется нормальным, если $\mathrm{lc}_1(g) = 1$ для всех элементов $g \in \Sigma$.

Лемма 3.4 (см. [12, Chap. 0, Lemma 15])**.** *Пусть A — бесконечное подмножество множества $\mathbb{N}^m \times \mathbb{N}_n$ $(m, n \in \mathbb{N},\ n \geqslant 1)$. Тогда существует бесконечная последовательность элементов множества A, строго возрастающая относительно порядка прямого произведения, в которой каждый элемент имеет одну и ту же проекцию на $\mathbb{N}_n$.*

Применяя последнюю лемму к множеству термов свободного $\mathscr{D}$-модуля E с базисом $\{e_1, \dots, e_k\}$, приходим к следующему результату.

Лемма 3.5. *Пусть E — свободный $\mathscr{D}$-модуль, рассмотренный выше, и пусть S — бесконечная последовательность термов множества Te. Тогда найдется индекс j $(1 \leqslant j \leqslant k)$ и бесконечная подпоследовательность $\tau_1 e_j, \dots, \tau_\nu e_j, \dots$ последовательности S такая, что $\tau_\nu | \tau_{\nu+1}$ для всех $\nu = 1, 2, \dots$.*

Теорема 3.6. *Всякое авторедуцированное подмножество свободного $\mathscr{D}$-модуля E конечно.*

Доказательство. Предположим, что Σ — бесконечное авторедуцированное подмножество E. Тогда Σ содержит бесконечное подмножество Σ_1 такое, что любые два элемента множества Σ_1 имеют различные 1-лидеры. В самом деле, если это не так, то существует бесконечное множество $\Sigma' \subseteq \Sigma$ такое, что все элементы множества Σ' имеют одинаковые 1-лидеры u. Согласно лемме 3.4 бесконечное множество

$$\{(\mathrm{ord}_2 u_f^{(2)}, \dots, \mathrm{ord}_p u_f^{(p)}) \in \mathbb{N}^{p-1} \mid f \in \Sigma'\}$$

содержит неубывающую бесконечную последовательность

$$(\operatorname{ord}_2 u_{f_1}^{(2)}, \dots, \operatorname{ord}_p u_{f_1}^{(p)}) \leqslant_P (\operatorname{ord}_2 u_{f_2}^{(2)}, \dots, \operatorname{ord}_p u_{f_2}^{(p)}) \leqslant_P \dots,$$

где $f_1, f_2, \dots \in \Sigma'$. Получаем, что всякий раз, когда $i > j$, f_i не редуцирован относительно f_j, что противоречит авторедуцированности множества Σ.

Таким образом, можно считать все 1-лидеры авторедуцированного множества Σ различными. Применяя лемму 3.5, получаем, что существует бесконечная последовательность $g_1, g_2, \dots$ элементов множества Σ таких, что $u_{g_i}^{(1)} | u_{g_{i+1}}^{(1)}$ для $i = 1, 2, \dots$. Пусть $k_{ij} = \operatorname{ord}_j u_{g_i}^{(1)}$ и $l_{ij} = \operatorname{ord}_j u_{g_i}^{(j)}$ $(2 \leqslant j \leqslant p)$. Очевидно, что $l_{ij} \geqslant k_{ij}$ $(i = 1, 2, \dots,\ j = 2, \dots, p)$, так что

$$\{(l_{i2} - k_{i2}, \dots, l_{ip} - k_{ip}) \mid i = 1, 2, \dots\} \subseteq \mathbb{N}^{p-1}.$$

Согласно лемме 3.4 найдется бесконечная последовательность индексов $i_1 < i_2 < \dots$ такая, что

$$(l_{i_1 2} - k_{i_1 2}, \dots, l_{i_1 p} - k_{i_1 p}) \leqslant_P (l_{i_2 2} - k_{i_2 2}, \dots, l_{i_2 p} - k_{i_2 p}) \leqslant_P \dots.$$

Тогда для каждого $j = 2, \dots, p$ имеем

$$\operatorname{ord}_j \left(\frac{u_{g_{i_2}}^{(1)}}{u_{g_{i_1}}^{(1)}} u_{g_{i_1}}^{(j)} \right) = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \leqslant k_{i_2 j} + l_{i_2 j} - k_{i_2 j} = l_{i_2 j} = \operatorname{ord}_j u_{g_{i_2}}^{(j)},$$

так что g_{i_2} содержит терм $\tau u_{g_{i_1}}^{(1)} = u_{g_{i_2}}^{(1)}$ такой, что $\operatorname{ord}_j(\tau u_{g_{i_1}}^{(j)}) \leqslant \operatorname{ord}_j u_{g_{i_2}}^{(j)}$ для $j = 2, \dots, p$. Таким образом, g_{i_2} не редуцирован относительно g_{i_1}, что противоречит авторедуцированности множества Σ. Это завершает доказательство теоремы. □

Теорема 3.7. *Пусть $\Sigma = \{g_1, \dots, g_r\}$ — авторедуцированное подмножество свободного $\mathscr{D}$-модуля E и $f \in E$. Тогда существует элемент $g \in E$ такой, что $f - g = \sum_{i=1}^{r} \lambda_i g_i$ для некоторых $\lambda_1, \dots, \lambda_r \in \mathscr{D}$ и g редуцирован относительно множества Σ.*

Доказательство. Если f редуцирован относительно множества Σ, то утверждение очевидно (можно положить $g = f$). Предположим, что f не редуцирован относительно Σ. В дальнейшем терм w_h, появляющийся в элементе $h \in E$, будет называться Σ-лидером для h, если w_h — наибольший (относительно порядка $<_1$) терм среди всех термов $\tau u_{g_j}^{(1)}$ $(\tau \in T,\ 1 \leqslant j \leqslant r)$, входящих в h и удовлетворяющих условию $\operatorname{ord}_\nu(\tau u_{g_j}^{(\nu)}) \leqslant \operatorname{ord}_\nu u_h^{(\nu)}$ при $\nu = 2, \dots, p$.

Пусть w_f — Σ-лидер элемента f и пусть c_f — коэффициент при w_f в f. Тогда $w_f = \tau u_{g_j}^{(1)}$ для некоторых $\tau \in T$ и j $(1 \leqslant j \leqslant r)$ таких, что $\operatorname{ord}_\nu(\tau u_{g_j}^{(\nu)}) \leqslant \operatorname{ord}_\nu u_f^{(\nu)}$ при $\nu = 2, \dots, p$. Без потери общности можно считать, что j соответствует максимальному (относительно упорядочения $<_1$) 1-лидеру $u_{g_j}^{(1)}$ в множестве всех соответствующих w_f 1-лидеров элементов множества Σ. Рассмотрим элемент $f' = f - \dfrac{c_f}{\tau(\operatorname{lc}_1(g_j))} \tau g_j$. Очевидно, f' не содержит w_f и $\operatorname{ord}_\nu(\tau u_{f'}^{(\nu)}) \leqslant \operatorname{ord}_\nu u_f^{(\nu)}$ при $\nu = 2, \dots, p$. Более того, f' не может содержать любой терм вида $\tau' u_{g_i}^{(1)}$ $(\tau' \in T,\ 1 \leqslant i \leqslant r)$, больший, чем w_f (относительно $<_1$) и удовлетворяющий условию $\operatorname{ord}_\nu(\tau' u_{g_i}^{(\nu)}) \leqslant \operatorname{ord}_\nu u_{f'}^{(\nu)}$ при $\nu = 2, \dots, p$. В самом деле, последнее неравенство влечет $\operatorname{ord}_\nu(\tau' u_{g_i}^{(\nu)}) \leqslant \operatorname{ord}_\nu u_f^{(\nu)}$ при $\nu = 2, \dots, p$, так что терм $\tau' u_{g_i}^{(1)}$ не может присутствовать в f. Этот терм не может также находиться и в τg_j, так как $u_{\tau g_j}^{(1)} = \tau u_{g_j}^{(1)} = w_f <_1 \tau' u_{g_i}^{(1)}$. Таким образом, $\tau' u_{g_i}^{(1)}$ не входит в $f' = f - \dfrac{c_f}{\tau(a_j)} \tau g_j$, следовательно Σ-лидер у f' строго меньше (относительно порядка $<_1$), чем Σ-лидер у f. Применяя ту же процедуру к элементу f' и продолжая рассуждать таким же способом, получаем элемент $g \in E$ такой, что $f - g$ есть линейная комбинация элементов $g_1, \dots, g_r$ с коэффициентами из $\mathscr{D}$ и g редуцирован относительно Σ. Это завершает доказательство. □

Процесс редукции, описанный в доказательстве теоремы 3.7, может быть представлен следующим алгоритмом.

Алгоритм 3.8. $(f, r, g_1, \dots, g_r; g)$

Вход: $f \in E$, натуральное число r, $\Sigma = \{g_1, \dots, g_r\} \subseteq E$, где $g_i \neq 0$, $i = 1, \dots, r$.

Выход: Элемент $g \in E$ и элементы $\lambda_1, \dots, \lambda_r \in R$, такие что $f = \lambda_1 g_1 + \dots + \lambda_r g_r$ и g редуцирован относительно Σ.

Начало

$\lambda_1 := 0$, …, $\lambda_r := 0$, $g := f$.

Пока существует i, $1 \leqslant i \leqslant r$, и терм w, входящий в g с ненулевым коэффициентом $c(w)$, такой, что $u_{g_i}^{(1)} | w$ и $\operatorname{ord}_k \left(\dfrac{w}{u_{g_i}^{(1)}} u_{g_i}^{(\nu)} \right) \leqslant \operatorname{ord}_\nu u_g^{(\nu)}$ при $\nu = 2, \dots, p$.

выполнять z:= наибольший (относительно $<_1$) терм в w, удовлетворяющий условию, приведенному выше.

j:= наименьшее число i, для которого $u_{g_i}^{(1)}$ — наибольший (относительно $<_1$) 1-лидер элемента $g_i \in \Sigma$ такой, что $u_{g_i}^{(1)} | z$ и $\operatorname{ord}_\nu \left(\dfrac{z}{u_{g_i}^{(1)}} u_{g_i}^{(\nu)} \right) \leqslant \operatorname{ord}_\nu u_g^{(\nu)}$ при $\nu = 2, \dots, p$,

$$\tau := \frac{z}{{u_{g_j}}^{(1)}}; \quad \lambda_j := \lambda_j + \frac{c(z)}{\tau(\operatorname{lc}_1(g_j))}\tau; \quad g := g - \frac{c(z)}{\tau(\operatorname{lc}_1(g_j))} g_j.$$

Конец

Определение 3.9. Пусть f и g — два элемента свободного векторного σ-K-пространства E. Будем говорить, что элемент f имеет меньший ранг, чем g, и писать $\operatorname{rk} f < \operatorname{rk} g$, если либо $u_f^{(1)} <_1 u_g^{(1)}$, либо существует некоторый индекс ν, $2 \leqslant \nu \leqslant p$, такой, что $u_f^{(\mu)} = u_g^{(\mu)}$ для $\mu = 1, \dots, \nu - 1$ и $u_f^{(\nu)} <_\nu u_g^{(\nu)}$. Если $u_f^{(i)} = u_g^{(i)}$ для $i = 1, \dots, p$, говорим, что f и g имеют один и тот же ранг и пишем $\operatorname{rk} f = \operatorname{rk} g$.

В дальнейшем, рассматривая авторедуцированные подмножества в E, всегда предполагаем, что их элементы упорядочены в порядке возрастания ранга. (Поэтому, если мы рассматриваем авторедуцированное множество $\Sigma = \{h_1, \dots, h_r\} \subseteq E$, то $\operatorname{rk} h_1 < \dots < \operatorname{rk} h_r$).

Определение 3.10. Пусть $\Sigma = \{h_1, \dots, h_r\}$ и $\Sigma' = \{h'_1, \dots, h'_s\}$ — два авторедуцированных подмножества свободного векторного σ-K-пространства E. Говорят, что авторедуцированное множество Σ имеет меньший ранг, чем Σ', если имеет место один из следующих случаев:

1) найдется $k \in \mathbb{N}$ такое, что $k \leqslant \min\{r, s\}$, $\operatorname{rk} h_i = \operatorname{rk} h'_i$ для $i = 1, \dots, k-1$ и $\operatorname{rk} h_k < \operatorname{rk} h'_k$;
2) $r > s$ и $\operatorname{rk} h_i = \operatorname{rk} h'_i$ при $i = 1, \dots, s$.

Если $r = s$ и $\operatorname{rk} h_i = \operatorname{rk} h'_i$ при $i = 1, \dots, r$, то говорят, что Σ имеет тот же ранг, что и Σ'.

Теорема 3.11. *В каждом непустом множестве авторедуцированных подмножеств свободного векторного σ-K-пространства E существует авторедуцированное подмножество наименьшего ранга.*

Доказательство. Пусть Φ — непустое множество авторедуцированных подмножеств модуля E. Определим по индукции бесконечно убывающую цепочку подмножеств в Φ следующим образом:

$$\Phi_0 = \Phi,$$

$$\Phi_1 = \left\{ \Sigma \in \Phi_0 \;\middle|\; \begin{array}{l} \Sigma \text{ содержит по крайней мере один элемент и первый} \\ \text{элемент в } \Sigma \text{ — наименьшего возможного ранга} \end{array} \right\}, \quad \dots,$$

$$\Phi_j = \left\{ \Sigma \in \Phi_{j-1} \;\middle|\; \begin{array}{l} \Sigma \text{ содержит по крайней мере } j \text{ элементов и } j\text{-й элемент} \\ \text{в } \Sigma \text{ — наименьшего возможного ранга} \end{array} \right\}, \dots.$$

Ясно, что если множество Φ_j непусто, то j-е элементы авторедуцированных множеств из Φ_j имеют одни и те же 1-лидеры $u_j^{(1)}$, одинаковые 2-лидеры $u_j^{(2)}$ и т. д. Если Φ_j непусты для всех $j = 1, 2, \dots$, то множество

$$\{f_j \mid f_j - j\text{-й элемент некоторого авторедуцированного множества из } \Phi_j\}$$

будет бесконечным авторедуцированным, что противоречит теореме 3.6. Поэтому найдется наименьший j такой, что Φ_j пусто. (Так как $\Phi_0 = \Phi$ непусто, то $j > 0$). Понятно, что каждый элемент множества Φ_{j-1} — авторедуцированное множество наименьшего ранга в Φ. □

Определение 3.12. Пусть N — $\mathscr{D}$-подмодуль свободного $\mathscr{D}$-модуля E. Тогда авторедуцированное подмножество модуля N, имеющее наименьший возможный ранг, называется *характеристическим множеством* модуля N.

Теорема 3.13. *Пусть N — $\mathscr{D}$-подмодуль свободного $\mathscr{D}$-модуля E и $\Sigma = \{g_1, \dots, g_r\}$ — характеристическое множество модуля N. Тогда элемент $f \in N$ редуцирован относительно Σ тогда и только тогда, когда $f = 0$.*

Доказательство. Предположим, что f — ненулевой элемент модуля N, редуцированный относительно Σ. Если $\operatorname{rk} f < \operatorname{rk} g_1$, то авторедуцированное множество $\{f\}$ имеет меньший ранг, чем Σ. Если $\operatorname{rk} g_1 < \operatorname{rk} f$ (f и g_1 не могут иметь один и тот же ранг, так как f редуцирован относительно Σ), то f и элементы $g \in \Sigma$, имеющие меньший ранг, чем f, составляют авторедуцированное множество меньшего ранга, чем Σ. В обоих случаям мы приходим к противоречию с тем, что Σ — характеристическое множество модуля N. □

Теорема 3.14. *Пусть N — циклический $\mathscr{D}$-подмодуль свободного $\mathscr{D}$-модуля E, порожденный элементом $g \in E$. Тогда $\{g\}$ — характеристическое множество модуля $N = \mathscr{D}g$.*

Доказательство. Пусть $h \in N$, так что h можно записать в виде $h = \sum_{i=1}^{m} c_i \tau_i g$, где $\tau_1, \dots, \tau_m \in T$, $c_1, \dots, c_m \in K$, $c_i \neq 0$ $(1 \leqslant i \leqslant m)$ и $\tau_i \neq \tau_j$, если $i \neq j$ $(1 \leqslant i, j \leqslant m)$. Ясно, что если τ_{r_i} — максимальный элемент множества $\{\tau_1, \dots, \tau_m\}$ относительно порядка $<_i$, то ${u_h}^{(i)} = \tau_{r_i} {u_g}^{(i)}$ $(1 \leqslant i \leqslant p)$. Мы видим, что h содержит кратное $\tau_{r_1} u_g^{(1)}$ для 1-лидера $u_g^{(1)}$, такое что

$$\operatorname{ord}_i(\tau_{r_1} {u_g}^{(i)}) \leqslant \operatorname{ord}_i(\tau_{r_i} {u_g}^{(i)}) = \operatorname{ord}_i u_h^{(i)}.$$

Поэтому h не редуцирован относительно g. Кроме того, так как

$$u_g^{(1)} \leqslant_1 \tau_{r_1} u_g^{(1)} = u_h^{(1)}, \quad {u_g}^{(i)} \leqslant_i \tau_i {u_g}^{(i)} = u_h^{(i)},$$

имеем $\operatorname{rk} g \leqslant \operatorname{rk} h$ и $\operatorname{rk} g = \operatorname{rk} h$ тогда и только тогда, когда $\tau_{r_i} = 1$ для $i = 1, \dots, m$, т.е. $h = cg$ для некоторого $c \in K$. Таким образом, N не содержит элементов, редуцированных относительно g, а g — элемент наименьшего ранга в N. Получаем, что если $\Sigma = \{h_1, \dots, h_l\}$ — характеристическое множество модуля N, то $\operatorname{rk} g = \operatorname{rk} h_1$ и $l = 1$, т.е. $\{g\}$ — также характеристическое множество модуля N. □

Теорема 3.15. *Пусть N — $\mathscr{D}$-подмодуль свободного $\mathscr{D}$-модуля E и пусть $\Sigma = \{g_1, \dots, g_r\}$ — характеристическое множество модуля N. Тогда элементы $g_1, \dots, g_r$ порождают $\mathscr{D}$-модуль N.*

Доказательство. Пусть f — произвольный элемент модуля N. Согласно теореме 3.7 существуют элементы $\lambda_1, \dots, \lambda_r \in \mathscr{D}$ и элемент $f' \in E$ такие, что f' редуцирован относительно Σ и $f - f' = \sum_{i=1}^{r} \lambda_i g_i$. Поэтому $f' \in N$ и теорема 3.13 показывает, что $f' = 0$, откуда $f = \sum_{i=1}^{r} \lambda_i g_i$. □

Теорема 3.16. *Пусть $\Sigma_1 = \{g_1, \dots, g_r\}$ и $\Sigma_2 = \{h_1, \dots, h_s\}$ — два нормальных характеристических множества некоторого $\mathscr{D}$-подмодуля N свободного $\mathscr{D}$-модуля E. Тогда $r = s$ и $g_i = h_i$ для всех $i = 1, \dots, r$.*

Доказательство. Так как Σ_1 и Σ_2 — два авторедуцированных множества одного (наименьшего возможного) ранга, $r = s$ и $u_{g_i}^{(\nu)} = u_{h_i}^{(\nu)}$ для $i = 1, \dots, r$, $\nu = 1, \dots, p$. Предположим, что существует i, $1 \leqslant i \leqslant r$, такое, что $g_i \neq h_i$. Полагая $f_i = g_i - h_i$, получаем, что $u_{f_i}^{(1)} <_1 u_{g_i}^{(1)}$ (так как коэффициенты у $u_{g_i}^{(1)}$ в g_i и h_i равны 1), $u_{f_i}^{(\nu)} \leqslant_\nu u_{g_i}^{(\nu)}$ $(2 \leqslant \nu \leqslant p)$ и f_i редуцирован относительно любого

элемента g_j ($1 \leqslant j \leqslant r$). В самом деле, предположим, что f_i содержит кратное $\tau u_{g_j}^{(1)}$ некоторого 1-лидера $u_{g_j}^{(1)}$ такое, что $\operatorname{ord}_\nu(\tau u_{g_j}^{(\nu)}) \leqslant \operatorname{ord}_\nu f_i^{(\nu)}$ при $\nu = 2, \dots, p$ (очевидно, f_i редуцирован относительно g_i, так что мы можем предположить, что $j \neq i$). Тогда по крайней мере один из элементов g_i, h_i должен содержать $\tau u_{g_j}^{(1)}$ и

$$\operatorname{ord}_\nu(\tau u_{g_j}^{(\nu)}) \leqslant \operatorname{ord}_\nu f_i^{(\nu)} \leqslant \operatorname{ord}_\nu u_{g_i}^{(\nu)} = \operatorname{ord}_\nu u_{h_i}^{(\nu)}$$

при $\nu = 2, \dots, p$, что противоречит тому, что множества Σ_1 и Σ_2 авторедуцированы. Теперь теорема 3.13 показывает, что $f_i = 0$, откуда $g_i = h_i$. Это завершает доказательство. □

4. Размерностные многочлены разностных векторных пространств

Ниже мы используем обозначения и соглашения предыдущего раздела. Мы начнем с факта, играющего решающую роль в доказательстве главного результата этой статьи, — теоремы о разностном размерностном многочлене от нескольких переменных разностного векторного пространства (см. ниже теорему 4.2).

Предложение 4.1. *Пусть K — разностное поле с базисным множеством $\sigma = \sigma_1 \cup \dots \cup \sigma_p$ (разбиение (1) фиксировано) и $\mathscr{D}$ — кольцо σ-операторов над K. Пусть M — конечно порожденный $\mathscr{D}$-модуль с системой порождающих $\{f_1, \dots, f_k\}$, E — свободный $\mathscr{D}$-модуль с базисом $e_1, \dots, e_k$ и $\pi : E \longrightarrow M$ — естественный $\mathscr{D}$-эпиморфизм E на M ($\pi(e_i) = f_i$ для $i = 1, \dots, k$). Кроме того, пусть $N = \operatorname{Ker}\pi$ и $\Sigma = \{g_1, \dots, g_d\}$ — характеристическое множество D-модуля N. Наконец, для каждых $r_1, \dots, r_p \in \mathbb{N}$ пусть $M_{r_1 \dots r_p} = \sum_{i=1}^{p} \mathscr{D}_{r_1 \dots r_p} f_i$ и пусть $U_{r_1 \dots r_p}$ обозначает множество $\{w \in Te \mid \operatorname{ord}_j w \leqslant r_j$ при $j = 1, \dots, p$ и либо w не является кратным никакого $u_{g_i}^{(1)}$ ($1 \leqslant i \leqslant d$), либо для всех $\tau \in T$, $g_i \in \Sigma$, таких, что $w = \tau u_{g_i}^{(1)}$, существует $j \in \{2, \dots, p\}$, такой что $\operatorname{ord}_j(\theta u_{g_j}^{(j)}) > r_j\}$. Тогда $\pi(U_{r_1 \dots r_p})$ — базис векторного K-пространства $M_{r_1 \dots r_p}$.*

Доказательство. Сначала докажем, что каждый элемент τf_i ($1 \leqslant i \leqslant q$, $\tau \in T(r_1, \dots, r_p)$), не принадлежащий $\pi(U_{r_1 \dots r_p})$, можно записать в виде конечной линейной комбинации элементов $\pi(U_{r_1 \dots r_p})$ с коэффициентами из K (так что множество $\pi(U_{r_1 \dots r_p})$ порождает K-векторное пространство $M_{r_1 \dots r_p}$). Так как $\tau f_i \notin \pi(U_{r_1 \dots r_p})$, имеем $\tau e_i \notin U_{r_1 \dots r_p}$, откуда $\tau e_i = \tau' u_{g_j}^{(1)}$ для некоторых $\tau' \in T$, $1 \leqslant j \leqslant d$, таких, что $\operatorname{ord}_\nu(\tau' u_{g_j}^{(\nu)}) \leqslant r_\nu$ ($\nu = 2, \dots, p$). Рассмотрим элемент $g_j = a_j u_{g_j}^{(1)} + \dots$ ($a_j \in K$, $a_j \neq 0$), где точки поставлены взамен других термов, присутствующих в g_j (очевидно, эти термы меньше, чем $u_{g_j}^{(1)}$, относительно порядка $<_1$). Так как $g_j \in N = \operatorname{Ker}\pi$, то $\pi(g_j) = a_j \pi(u_{g_j}^{(1)}) + \dots = 0$, откуда

$$\pi(\tau' g_j) = a_j \pi(\tau' u_{g_j}^{(1)}) + \dots = a_j \pi(\tau e_i) + \dots = a_j \tau f_i + \dots = 0,$$

так что τf_i — конечная линейная комбинация с коэффициентами из K некоторых элементов $\tilde{\tau} f_l$ ($1 \leqslant l \leqslant k$) таких, что $\tilde{\tau} \in T(r_1, \dots, r_p)$ и $\tilde{\tau} e_l <_1 \tau' u_{g_j}^{(1)}$. (Отметим, что $\operatorname{ord}_1 \tilde{\tau} \leqslant r_1$, так как $\tilde{\tau} e_l <_1 \tau e_i$ и $\tau \in T(r_1, \dots, r_p)$; $\operatorname{ord}_\nu \tilde{\tau} \leqslant r_\nu$ ($\nu = 2, \dots, p$), поскольку $\tilde{\tau} e_l \leqslant_\nu u_{\tau' g_j}^{(\nu)} = \tau' u_{g_j}^{(\nu)}$ и $\operatorname{ord}_\nu(\tau' u_{g_j}^{(\nu)}) \leqslant r_\nu$.) Таким образом, мы можем применить индукцию по τe_j ($\tau \in T$, $1 \leqslant j \leqslant k$) относительно порядка $<_1$ и получить, что каждый элемент τf_i ($\tau \in T(r_1, \dots, r_p)$, $1 \leqslant j \leqslant k$) можно записать в виде конечной линейной комбинации элементов из $\pi(U_{r_1 \dots r_p})$ с коэффициентами из поля K.

Теперь докажем, что множество $\pi(U_{r_1 \dots r_p})$ линейно независимо над K. Предположим, что $\sum_{i=1}^{m} a_i \pi(u_i) = 0$ для некоторых $u_1, \dots, u_m \in U_{r_1 \dots r_p}$, $a_1, \dots, a_k \in K$. Тогда $h = \sum_{i=1}^{m} a_i u_i$ — элемент из N, редуцированный относительно Σ. В самом деле, если терм $u = \tau e_j$ имеется в h (так что $u = u_i$ для некоторого $i = 1, \dots, m$), то либо u не кратен никакому из $u_{g_\nu}^{(1)}$ ($1 \leqslant \nu \leqslant d$), либо $u = \tau u_{g_\nu}^{(1)}$ для некоторых $\tau \in T$, $1 \leqslant \nu \leqslant d$, таких, что $\operatorname{ord}_\mu(\tau u_{g_\nu}^{(\mu)}) > r_\mu \geqslant \operatorname{ord}_\mu u_h^{(\mu)}$ для некоторого

μ, $2 \leqslant \mu \leqslant p$. Согласно теореме 3.13 получаем $h = 0$, откуда $a_1 = \cdots = a_m = 0$. Это завершает доказательство предложения. □

Теорема 4.2. *Пусть K — разностное поле с базисным множеством $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ и $\mathscr{D}$ — кольцо разностных операторов над K, снабженное стандартной p-мерной фильтрацией, соответствующей разбиению* (1) *множества σ. Кроме того, пусть $n_i = \operatorname{Card} \sigma_i$ $(i = 1, \ldots, p)$ и $\{M_{r_1 \ldots r_p} \mid (r_1, \ldots, r_p) \in \mathbb{Z}^p\}$ — отличная p-мерная фильтрация векторного σ-K-пространства M. Тогда существует многочлен $\phi(t_1, \ldots, t_p) \in \mathbb{Q}[t_1, \ldots, t_p]$ такой, что*

(i) $\phi(r_1, \ldots, r_p) = \dim_K M_{r_1 \ldots r_p}$ *для всех достаточно больших* $(r_1, \ldots, r_p) \in \mathbb{Z}^p$;
(ii) $\deg_{t_i} \phi \leqslant n_i$ $(1 \leqslant i \leqslant p)$, *так что* $\deg \phi \leqslant n$ *и многочлен $\phi(t_1, \ldots, t_p)$ можно представить в виде*

$$\phi(t_1, \ldots, t_p) = \sum_{i_1=0}^{n_1} \cdots \sum_{i_p=0}^{n_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \ldots \binom{t_p + i_p}{i_p},$$

где $a_{i_1 \ldots i_p} \in \mathbb{Z}$ для всех $i_1, \ldots, i_p$.

Доказательство. Так как p-мерная фильтрация $\{M_{r_1 \ldots r_p} \mid (r_1, \ldots, r_p) \in \mathbb{Z}^p\}$ является отличной, найдется элемент $(h_1, \ldots, h_p) \in \mathbb{Z}^p$ такой, что $\mathscr{D}_{r_1, \ldots, r_p} M_{h_1, \ldots, h_p} = M_{r_1 + h_1, \ldots, r_p + h_p}$ для всех $(r_1, \ldots, r_p) \in \mathbb{N}^p$. Кроме того, $M_{h_1, \ldots, h_p}$ — конечномерное векторное K-пространство и любой его базис порождает M как левый $\mathscr{D}$-модуль. Получаем, что $M = \sum_{i=1}^{k} \mathscr{D} y_i$ для некоторых элементов $y_1, \ldots, y_q \in M$.

Пусть E — свободный $\mathscr{D}$-модуль с базисом $e_1, \ldots, e_q$, N — ядро естественного σ-эпиморфизма $\pi : E \to M$ $(\pi(e_i) = y_i$ для $i = 1, \ldots, q)$ и множество $U_{r_1 \ldots r_p}$ $(r_1, \ldots, r_p \in \mathbb{N})$ — такое же, как в условиях предложения 4.1. Кроме того, пусть $\Sigma = \{g_1, \ldots, g_d\}$ — характеристическое множество модуля N. Согласно предложению 4.1 для любых $r_1, \ldots, r_p \in \mathbb{N}$ множество $\pi(U_{r_1, \ldots, r_p})$ является базисом векторного K-пространства $M_{r_1, \ldots, r_p}$. Поэтому

$$\dim_K M_{r_1, \ldots, r_p} = \operatorname{Card} \pi(U_{r_1, \ldots, r_p}) = \operatorname{Card} U_{r_1, \ldots, r_p}.$$

(Во второй части доказательства предложения 4.1 было показано, что ограничение отображения π на $U_{r_1, \ldots, r_p}$ биективно.)

Пусть $U'_{r_1, \ldots, r_p} = \{w \in U_{r_1, \ldots, r_p} \mid w$ не кратен никакому элементу u_{g_i} $(1 \leqslant i \leqslant d)\}$ и пусть $U''_{r_1, \ldots, r_p} = \{w \in U_{r_1, \ldots, r_p} |$ существуют $g_j \in \Sigma$ и $\tau \in T$ такие, что $w = \tau u^{(1)}_{g_j}$ и $\operatorname{ord}_\nu(\tau u^{(\nu)}_{g_j}) > r_\nu$ для некоторого ν, $2 \leqslant \nu \leqslant p\}$. Тогда

$$U_{r_1, \ldots, r_p} = U'_{r_1, \ldots, r_p} \cup U''_{r_1, \ldots, r_p}, \quad U'_{r_1, \ldots, r_p} \cap U''_{r_1, \ldots, r_p} = \emptyset,$$

откуда

$$\operatorname{Card} U_{r_1, \ldots, r_p} = \operatorname{Card} U'_{r_1, \ldots, r_p} + \operatorname{Card} U''_{r_1, \ldots, r_p}.$$

Согласно теореме 2.7 существует целозначный многочлен $\omega(t_1, \ldots, t_p)$ от p переменных $t_1, \ldots t_p$ такой, что $\omega(r_1, \ldots, r_p) = \operatorname{Card} U'_{r_1, \ldots, r_p}$ для всех достаточно больших $(r_1, \ldots, r_p) \in \mathbb{N}^p$. Для того, чтобы выразить $\operatorname{Card} U''_{r_1, \ldots, r_p}$ в терминах $r_1, \ldots, r_p$, положим $a_{ij} = \operatorname{ord}_i u^{(1)}_{g_j}$ и $b_{ij} = \operatorname{ord}_i u^{(i)}_{g_j}$, $i = 1, \ldots, p$, $j = 1, \ldots, d$. Очевидно, $a_{1j} = b_{1j}$ и $a_{ij} \leqslant b_{ij}$ для $i = 1, \ldots, p$, $j = 1, \ldots, d$. Далее, для любых $\mu = 1, \ldots, p$ и целых $k_1, \ldots, k_\mu$ таких, что $2 \leqslant k_1 < \cdots < k_\mu \leqslant p$, положим $V_{j; k_1, \ldots, k_\mu}(r_1, \ldots, r_p) = \{\tau u^{(1)}_{g_j} \mid \operatorname{ord}_i \tau \leqslant r_i - a_{ij}$ для $i = 1, \ldots, p$ и $\operatorname{ord}_\nu \tau > r_\nu - b_{\nu j}$ тогда и только тогда, когда ν равно одному из чисел $k_1, \ldots, k_\mu\}$.

Тогда $\operatorname{Card} V_{j;k_1,\dots,k_\mu}(r_1,\dots,r_p) = \phi_{j;k_1,\dots,k_\mu}(r_1,\dots,r_p)$, где $\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p)$ — целозначный многочлен от p переменных $t_1,\dots,t_p$, определенный формулой

$$\begin{aligned}\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p) = \binom{t_1+n_1-b_{1j}}{n_1}\dots\binom{t_{k_1-1}+n_{k_1-1}-b_{k_1-1,j}}{n_{k_1-1}}\\ \left[\binom{t_{k_1}+n_{k_1}-a_{k_1,j}}{n_{k_1}}-\binom{t_{k_1}+n_{k_1}-b_{k_1,j}}{n_{k_1}}\right]\binom{t_{k_1+1}+n_{k_1+1}-b_{k_1+1,j}}{n_{k_1+1}}\\ \dots\binom{t_{k_q-1}+n_{k_q-1}-b_{k_q-1,j}}{n_{k_q-1}}\left[\binom{t_{k_q}+n_{k_q}-a_{k_q,j}}{n_{k_q}}-\binom{t_{k_q}+n_{k_q}-b_{k_q,j}}{n_{k_q}}\right]\\ \dots\binom{t_p+n_p-b_{pj}}{n_p}.\end{aligned} \tag{5}$$

(Из пункта (iii) теоремы 2.7 следует, что

$$\operatorname{Card}\left\{\tau\in T \;\middle|\; \operatorname{ord}_1\tau\leqslant r_1,\dots,\operatorname{ord}_p\tau\leqslant r_p\right\} = \prod_{i=1}^{p}\binom{r_i+n_i}{n_i}$$

для всех $r_1,\dots,r_p\in\mathbb{N}$). Легко видеть, что $\deg_{t_i}\phi_{j;k_1,\dots,k_\mu}\leqslant n_i$ для $i=1,\dots,p$.

Теперь для любых $j=1,\dots,d$ положим $V_j(r_1,\dots,r_p)=\{\tau u_j^{(1)} \mid \operatorname{ord}_i\tau\leqslant r_i-a_{ij}$ для $i=1,\dots,p$ и существует $\nu\in\mathbb{N}$, $2\leqslant\nu\leqslant p$, такое, что $\operatorname{ord}_\nu\tau > r_\nu - b_{\nu j}\}$. Тогда комбинаторный принцип включения-исключения влечет $\operatorname{Card} V_j(r_1,\dots,r_p)=\phi_j(r_1,\dots,r_p)$, где $\phi_j(t_1,\dots,t_p)$ — целозначный многочлен от p переменных $t_1,\dots,t_p$, определенный по формуле

$$\begin{aligned}\phi_j(t_1,\dots,t_p) = \sum_{k_1=1}^{p}\phi_{j;k_1}(t_1,\dots,t_p) - \sum_{1\leqslant k_1<k_2\leqslant p}\phi_{j;k_1,k_2}(t_1,\dots,t_p)+\dots+\\ +(-1)^{\mu-1}\sum_{1\leqslant k_1<\dots k_\mu\leqslant p}\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p)+\dots+(-1)^{p-1}\phi_{j;2,\dots,p}(t_1,\dots,t_p).\end{aligned}$$

Легко видеть, что $\deg_{t_i}\phi_j(t_1,\dots,t_p)\leqslant n_i$ для $i=1,\dots,p$.

Применяя принцип включения-исключения, мы получаем, что

$$\begin{aligned}\operatorname{Card} U''_{r_1\dots r_p} = \operatorname{Card}\bigcup_{j=1}^{d}V_j(r_1,\dots,r_p) = \sum_{j=1}^{d}\operatorname{Card} V_j(r_1,\dots,r_p) -\\ -\sum_{1\leqslant j_1<j_2\leqslant d}\operatorname{Card}(V_{j_1}(r_1,\dots,r_p)\bigcap V_{j_2}(r_1,\dots,r_p))+\dots+\\ +(-1)^{d-1}\operatorname{Card}\bigcap_{\nu=1}^{d}V_{j_\nu}(r_1,\dots,r_p),\end{aligned}$$

так что достаточно доказать, что для всех $s=1,\dots,d$ и для любых индексов $j_1,\dots,j_s$, $1\leqslant j_1<\dots<j_s\leqslant d$, имеем

$$\operatorname{Card}(V_{j_1}(r_1,\dots,r_p)\cap\dots\cap V_{j_s}(r_1,\dots,r_p)) = \phi_{j_1,\dots,j_s}(r_1,\dots,r_p),$$

где $\phi_{j_1,\dots,j_s}(t_1,\dots,t_p)$ — целозначный многочлен от p переменных $t_1,\dots,t_p$ такой, что $\deg_{t_i}\phi_{j_1,\dots,j_s}\leqslant n_i$ для $i=1,\dots,p$. Ясно, что пересечение $V_{j_1}(r_1,\dots,r_p)\cap\dots\cap V_{j_s}(r_1,\dots,r_p)$ непусто (и значит, $\phi_{j_1,\dots,j_s}\neq 0$) тогда и только тогда, когда лидеры $u_{g_{j_1}}^{(1)},\dots,u_{g_{j_s}}^{(1)}$ содержат один и тот же элемент e_i ($1\leqslant i\leqslant q$). Рассмотрим такое пересечение $V_{j_1}(r_1,\dots,r_p)\cap\dots\cap V_{j_s}(r_1,\dots,r_p)$, пусть $v(j_1,\dots,j_s)=\operatorname{lcm}(u_{j_1}^{(1)},\dots,u_{j_s}^{(1)})$ и пусть $v(j_1,\dots,j_s)=\gamma_\nu u_{g_{j_\nu}}$ ($1\leqslant\nu\leqslant s$, $\gamma_1,\dots,\gamma_s\in T$). Тогда $V_{j_1}(r_1,\dots,r_p)\cap\dots\cap V_{j_s}(r_1,\dots,r_p)$ — множество всех термов $u=\tau v(j_1,\dots,j_s)$ таких, что $\operatorname{ord}_i u\leqslant r_i$ (т.е. $\operatorname{ord}_i\tau\leqslant r_i-\operatorname{ord}_i v(j_1,\dots,j_s)$) для $i=1,\dots,p$ и для любых $l=1,\dots,s$, найдется по крайней мере один

индекс $\nu \in \{2, \dots, p\}$ такой, что $\operatorname{ord}_\nu(\tau\gamma_l u^{(\nu)}_{g_{j_l}}) > r_\nu$, т.е.

$$\operatorname{ord}_\nu \tau > r_\nu - \operatorname{ord}_\nu v(j_1, \dots, j_s) - \operatorname{ord}_\nu u^{(\nu)}_{g_{j_l}} + \operatorname{ord}_\nu u^{(1)}_{g_{j_l}}.$$

Обозначая $\operatorname{ord}_i v(j_1, \dots, j_s)$ через $c^{(i)}_{j_1,\dots,j_s}$ $(1 \leqslant i \leqslant p)$ и применяя принцип включения-исключения снова, мы получаем, что $\operatorname{Card} \bigcap_{\mu=1}^{s} V_{j_\mu}(r_1, \dots, r_p)$ — альтернированная сумма термов вида $\operatorname{Card} W(j_1, \dots, j_s; k_{11}, k_{12}, \dots, k_{1q_1}, k_{21}, \dots, k_{sq_s}; r_1, \dots, r_p)$, где $W(j_1, \dots, j_s;\ k_{11}, k_{12}, \dots, k_{1q_1}, k_{21}, \dots, k_{sq_s};\ r_1, \dots, r_p) = \{\tau \in T \mid \operatorname{ord}_i \tau \leqslant r_i - c^{(i)}_{j_1,\dots,j_s}$ для $i = 1, \dots, p$, для любого $l = 1, \dots, s$ неравенство $\operatorname{ord}_k \tau > r_k - c^{(k)}_{j_1,\dots,j_s} + a_{kj_l} - b_{kj_l}$ выполняется тогда и только тогда, когда $k = k_{li}$ для некоторого $i = 1, \dots, q_l\}$ ($q_1, \dots, q_s$ — некоторые натуральные числа из множества $\{1, \dots, p\}$, а $\{k_{i\mu} \mid 1 \leqslant i \leqslant s,\ 1 \leqslant \mu \leqslant q_s\}$ — семейство целых чисел таких, что $2 \leqslant k_{i1} < k_{i2} < \dots < k_{iq_i} \leqslant p$ для $i = 1, \dots, s$). Таким образом, достаточно показать, что

$$\operatorname{Card} W(j_1, \dots, j_s; k_{11}, \dots, k_{sq_s}; r_1, \dots, r_p) = \psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(r_1, \dots, r_p),$$

где $\psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(t_1, \dots, t_p)$ — целозначный многочлен от p переменных $t_1, \dots, t_p$ такой, что $\deg_i \psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}} \leqslant n_i$ $(i = 1, \dots, p)$. Но это почти очевидно: как и в процессе вычисления значения $\operatorname{Card} V_{j;k_1,\dots,k_q}(r_1, \dots, r_p)$ (где используется теорема 2.7(iii) для получения формулы (5)), мы видим, что $\operatorname{Card} W(j_1, \dots, j_s; k_{11}, \dots, k_{sq_s}; r_1, \dots, r_p)$ — произведение термов вида

$$\binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S_\nu}{n_\nu}$$

(такой терм соответствует числу $\nu \in \{1, \dots, p\}$, отличному от всех $k_{i\mu}$ $(1 \leqslant i \leqslant s,\ 1 \leqslant \mu \leqslant q_s)$; S_ν определено как $\max\{b_{\nu j_l} - a_{\nu j_l} \mid 1 \leqslant l \leqslant s\}$) и термов вида

$$\left[\binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s}}{n_\nu} - \binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S'_\nu}{n_\nu}\right]$$

(такой терм содержится в произведении, если $\nu = k_{i\mu}$ для некоторого i, μ; если $k_{i_1\mu_1}, \dots, k_{i_e\mu_e}$ — все элементы множества $\{k_{i\mu} \mid 1 \leqslant i \leqslant s, 1 \leqslant \mu \leqslant q_s\}$, равные ν $(1 \leqslant e \leqslant s,\ 1 \leqslant i_1 < \dots < i_e \leqslant s)$, тогда S'_ν определено как $\min\{b_{\nu j_{i_\lambda}} - a_{\nu j_{i_\lambda}} \mid 1 \leqslant \lambda \leqslant l\}$). Соответствующий целозначный многочлен $\psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(t_1, \dots, t_p)$ является произведением p «элементарных» целозначных многочленов, каждый из которых равен либо $\binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S_\nu}{n_\nu}$, либо $\left[\binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s}}{n_\nu} - \binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S'_\nu}{m_\nu}\right]$ $(1 \leqslant \nu \leqslant p)$. Так как степень этого произведения относительно каждой переменной t_i $(1 \leqslant i \leqslant p)$ не превосходит n_i, то это завершает доказательство теоремы. □

Определение 4.3. Многочлен $\phi(t_1, \dots, t_p)$, существование которого установлено в теореме 4.2, называется $(\sigma_1, \dots, \sigma_p)$-размерностным многочленом σ-K-векторного пространства M, ассоциированным с p-мерной фильтрацией $\{M_{r_1\dots r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$.

Пример 4.4. В обозначениях в теоремы 4.2 положим $n = 2$, $\sigma_1 = \{\alpha_1\}$, $\sigma_2 = \{\alpha_2\}$, и пусть векторное σ-K-пространство M порождено одним элементом x, удовлетворяющим определяющему уравнению

$$\alpha_1 x + \alpha_2^2 x + x = 0.$$

Другими словами, M — фактормодуль свободного $\mathscr{D}$-модуля $E = \mathscr{D}e$ со свободным образующим e по его $\mathscr{D}$-подмодулю $N = \mathscr{D}(\alpha_1 + \alpha_2^2 + 1)e$. Согласно теореме 3.14 нормальное характеристическое

множество модуля N состоит из одного элемента $g = (\alpha_1 + \alpha_2^2 + 1)e$. В ходе доказательства теоремы 4.2 показано, что (σ_1, σ_2)-размерностный многочлен для M, ассоциированный с естественной бифильтрацией

$$\left(M_{rs} = \sum_{i=0}^{r} \sum_{j=0}^{s} K\alpha_1^i \alpha_2^j x \right)_{r,s \in \mathbb{N}},$$

таков:

$$\phi(t_1, t_2) = \left[\binom{t_1+1}{1} \binom{t_2+1}{1} - \binom{t_1}{1} \binom{t_2+1}{1} \right] + \binom{t_1}{1} \left[\binom{t_2+1}{1} - \binom{t_2-1}{1} \right] = 2t_1 + t_2 + 1.$$

(В обозначениях доказательства теоремы многочлен в первых скобках дает $\operatorname{Card} U'_{rs}$, тогда как многочлен

$$\binom{t_1}{1} \left[\binom{t_2+1}{1} - \binom{t_2-1}{1} \right]$$

дает $\operatorname{Card} U''_{rs}$ для всех достаточно больших $(r, s) \in \mathbb{N}^2$.)

Для любой перестановки $(j_1, \dots, j_p)$ множества $\{1, \dots, p\}$ определим лексикографический порядок $\leqslant_{j_1,\dots,j_p}$ на $\mathbb{N}^p$ так: $(r_1, \dots, r_p) \leqslant_{j_1,\dots,j_p} (s_1, \dots, s_p)$ тогда и только тогда, когда либо $r_{j_1} < s_{j_1}$, либо существует $k \in \mathbb{N}$, $1 \leqslant k \leqslant p-1$, такое, что $r_{j_\nu} = s_{j_\nu}$ для $\nu = 1, \dots, k$ и $r_{j_{k+1}} < s_{j_{k+1}}$. Теперь, если $\Sigma \subseteq \mathbb{N}^p$, то Σ' будет обозначать множество $\{e \in \Sigma \mid e$ — максимальный элемент в Σ относительно одного из $p!$ лексикографических порядков $\leqslant_{j_1,\dots,j_p}\}$.

Пример 4.5. Пусть $\Sigma = \{(3,0,2), (2,1,1), (0,1,4), (1,0,3), (1,1,6), (3,1,0), (1,2,0)\} \subseteq \mathbb{N}^3$. Тогда $\Sigma' = \{(3,0,2), (3,1,0), (1,1,6), (1,2,0)\}$.

Следующий результат является следствием того факта, что если $\{M_{r_1\dots r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$ и $\{M'_{r_1\dots r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$ — две отличные p-мерные фильтрации одного и того же конечно порожденного векторного σ-K-пространства M, то существует элемент $(s_1, \dots, s_p) \in \mathbb{N}^p$ такой, что $M_{r_1\dots r_p} \subseteq M'_{r_1+s_1,\dots,r_p+s_p}$ и $M'_{r_1\dots r_p} \subseteq M_{r_1+s_1,\dots,r_p+s_p}$ для всех достаточно больших $(r_1, \dots, r_p) \in \mathbb{Z}^p$.

Теорема 4.6. *Пусть K — разностное (σ-) поле, M — конечно порожденное векторное σ-K-пространство, $\{M_{r_1\dots r_p} \mid (r_1, \dots, r_p) \in \mathbb{Z}^p\}$ — отличная p-мерная фильтрация на M и*

$$\phi(t_1, \dots, t_p) = \sum_{i_1=0}^{n_1} \cdots \sum_{i_p=0}^{n_p} a_{i_1\dots i_p} \binom{t_1+i_1}{i_1} \dots \binom{t_p+i_p}{i_p}$$

— размерностный многочлен, ассоциированный с этой фильтрацией. Пусть

$$\Sigma = \{(i_1, \dots, i_p) \in \mathbb{N}^p \mid 0 \leqslant i_k \leqslant n_k \ (k = 1, \dots, p) \text{ и } a_{i_1\dots i_p} \neq 0\}.$$

Тогда $d = \deg \phi$, $a_{n_1\dots n_p}$, элементы $(k_1, \dots, k_p) \in \Sigma'$, соответствующие коэффициенты $a_{k_1\dots k_p}$ и коэффициенты термов полной степени d не зависят от выбора совершенной фильтрации.

5. Размерностные многочлены расширений разностных полей

Пусть K — инверсное разностное поле, базисное множество $\sigma = \{\alpha_1, \dots, \alpha_n\}$ которого представляет собой дизъюнктное объединение p конечных множеств ($p \geqslant 1$): $\sigma = \sigma_1 \cup \dots \cup \sigma_p$, где $\sigma_1 = \{\alpha_1, \dots, \alpha_{n_1}\}$, $\sigma_2 = \{\alpha_{n_1+1}, \dots, \alpha_{n_1+n_2}\}$, $\dots$, $\sigma_p = \{\alpha_{n_1+\dots+n_{p-1}+1}, \dots, \alpha_n\}$ ($n_1, \dots, n_p \in \mathbb{N}$). В дальнейшем мы сохраняем обозначения раздела 2. В частности, T обозначает свободную абелеву полугруппу, порожденную σ, и для любых $(r_1, \dots, r_p) \in \mathbb{N}^p$ полагаем $T(r_1, \dots, r_p) = \{\tau \in T \mid \operatorname{ord}_i \tau \leqslant r_i$ при $i = 1, \dots, p\}$. Более того, $K\{y_1, \dots, y_m\}$ обозначает алгебру σ-многочленов от σ-неизвестных $y_1, \dots, y_m$ над K. До конца статьи элементы $\tau y_i \in K\{y_1, \dots, y_m\}$ ($\tau \in T$, $1 \leqslant i \leqslant m$) называем *термами* (тот факт, что это слово было использовано в разделе 4 для определенных элементов свободного разностного векторного пространства, не вызывает недоразумений), тогда как элементы множества T продолжаем называть мономами. Множества всех термов обозначается

TY и рассматривается вместе с p порядками, соответствующими порядкам полугруппы T, введенной в разделе 2 (они обозначаются теми же символами $<_1, \dots, <_p$). Эти порядки определяются следующим образом: $\tau y_j <_i \tau' y_k$ ($\tau, \tau' \in T$, $1 \leqslant j, k \leqslant m$, $1 \leqslant i \leqslant p$) тогда и только тогда, когда $\tau <_i \tau'$ или $\tau = \tau'$ и $j < k$.

i-м порядком терма $u = \tau y_j$ ($1 \leqslant i \leqslant p$, $\theta \in T$, $1 \leqslant j \leqslant m$) называется число $\operatorname{ord}_i u = \operatorname{ord}_i \tau$. Число $\operatorname{ord} u = \operatorname{ord} \tau$ называется порядком терма u.

Говорят, что терм $u = \tau y_i$ делится на терм $v = \tau' y_j$ и пишут $v|u$, если $i = j$ и $\tau'|\tau$. Для любых термов $u_1 = \tau_1 y_j, \dots, u_q = \tau_q y_j$, содержащих одну и ту же σ-переменную y_j ($1 \leqslant j \leqslant m$), терм $\operatorname{lcm}(\tau_1, \dots, \tau_q) y_j$ называется наименьшим общим кратным $u_1, \dots, u_q$ и обозначается через $\operatorname{lcm}(u_1, \dots, u_q)$.

Если $A \in K\{y_1, \dots, y_m\}$, $A \notin K$ и $1 \leqslant i \leqslant p$, то наибольший в смысле порядка $<_i$ терм, присутствующий в A, называется i-м лидером σ-многочлена A и обозначается через $u_A^{(i)}$. Если A представить как многочлен от одной переменной $u_A^{(1)}$,

$$A = I_d (u_A^{(1)})^d + I_{d-1} (u_A^{(1)})^{d-1} + \dots + I_0$$

(σ-многочлены I_d, I_{d-1}, $\dots$, I_0 не содержат $u_A^{(1)}$), то I_d называется *старшим коэффициентом* σ-многочлена A и обозначается через I_A.

Пусть A и B — два σ-многочлена из $K\{y_1, \dots, y_m\}$. Будем говорить, что A *имеет меньший ранг, чем* B, и писать $\operatorname{rk} A < \operatorname{rk} B$, если либо $A \in K$, $B \notin K$, либо вектор $(u_A^{(1)}, \deg_{u_A^{(1)}} A, \operatorname{ord}_2 u_A^{(2)}, \dots, \operatorname{ord}_p u_A^{(p)})$ меньше вектора $(u_B^{(1)}, \deg_{u_B^{(1)}} B, \operatorname{ord}_2 u_B^{(2)}, \dots, \operatorname{ord}_p u_B^{(p)})$ относительно лексикографического порядка (здесь $u_A^{(1)}$ и $u_B^{(1)}$ сравниваются относительно $<_1$, а все другие координаты векторов сравниваются относительно естественного порядка на $\mathbb{N}$). Если эти два вектора равны (или $A \in K$ и $B \in K$), то мы говорим, что σ-многочлены A и B имеют одинаковый ранг и пишем $\operatorname{rk} A = \operatorname{rk} B$.

Пусть K — разностное (σ-) поле и L — конечно порожденное σ-расширение поля K с порождающими $\eta = \{\eta_1, \dots, \eta_m\}$, т.е. $L = K\langle \eta_1, \dots, \eta_m \rangle$. Тогда существует естественный σ-гомоморфизм ϕ_η кольца σ-многочленов $K\{y_1, \dots, y_m\}$ на σ-подкольцо $K\{\eta_1, \dots, \eta_m\}$ поля L такой, что $\phi_\eta(a) = a$ для любых $a \in K$ и $\phi_\eta(y_j) = \eta_j$ для $j = 1, \dots, m$. Если A — σ-многочлен из $K\{y_1, \dots, y_m\}$, то элемент $\phi_\eta(A)$ называется *значением* A в η и обозначается через $A(\eta)$. Очевидно, что ядро P σ-гомоморфизма ϕ_η — простой рефлексивный σ-идеал кольца $K\{y_1, \dots, y_m\}$. Этот идеал называется *определяющим* идеалом для η над K или определяющим идеалом σ-расширения поля $K\langle \eta_1, \dots, \eta_n \rangle / K$. Легко видеть, что если поле частных Q факторкольца $\bar{R} = K\{y_1, \dots, y_n\}/P$ рассмотреть как σ-поле (где $\alpha(\frac{u}{v}) = \frac{\alpha(u)}{\alpha(v)}$ для всех $u, v \in \bar{R}$), то это поле частных естественным образом σ-изоморфно полю L. (σ-Изоморфизм Q на L оставляет на месте элементы поля K и отображает образы σ-неизвестных $y_1, \dots, y_m$ в фактор-кольце $\bar{R}$ на элементы $\eta_1, \dots, \eta_m$ соответственно.)

Определение 5.1. Пусть A и B — два σ-многочлена из $K\{y_1, \dots, y_m\}$, $A \notin K$. σ-Многочлен B называется редуцированным относительно A, если B не содержит степеней $(\tau u_A^{(1)})^k$ ($\tau \in T$, $k \in \mathbb{N}$) таких, что $k \geqslant \deg_{u_A^{(1)}} A$ и $\operatorname{ord}_i(\tau u_A^{(i)}) \leqslant \operatorname{ord}_i u_B^{(i)}$ для $i = 2, \dots, p$.

σ-Многочлен B называется редуцированным относительно множества $\Sigma \subseteq K\{y_1, \dots, y_m\}$, если B редуцирован относительно всех элементов Σ.

Определение 5.2. Множество σ-многочленов $\Sigma \subseteq K\{y_1, \dots, y_m\}$ называется авторедуцированным, если $\Sigma \cap K = \emptyset$ и каждый элемент Σ редуцирован относительно всех остальных.

Доказательство следующего утверждения аналогично доказательству теоремы 3.6.

Теорема 5.3. *Каждое авторедуцированное множество σ-многочленов конечно.*

Начиная с этого момента, рассматривая авторедуцированные множества в кольце $K\{y_1,\dots,y_m\}$, предполагаем, что их элементы упорядочены по возрастанию ранга. (Следовательно, если мы рассматриваем авторедуцированное множество Δ-многочленов $\Sigma=\{A_1,\dots,A_r\}$, то $\operatorname{rk}A_1<\dots<\operatorname{rk}A_r$.)

Определение 5.4. Пусть $\Sigma=\{A_1,\dots,A_r\}$ и $\Sigma'=\{B_1,\dots,B_s\}$ — два авторедуцированных множества в кольце разностных многочленов $K\{y_1,\dots,y_n\}$. Авторедуцированное множество Σ имеет меньший ранг, чем Σ', если выполнено одно из следующих условий:

1) найдется $k\in\mathbb{N}$ такое, что $k\leqslant\min\{r,s\}$, $\operatorname{rk}A_i=\operatorname{rk}B_i$ для $i=1,\dots,k-1$, и $\operatorname{rk}A_k<\operatorname{rk}B_k$;
2) $r>s$ и $\operatorname{rk}A_i=\operatorname{rk}B_i$ для $i=1,\dots,s$.

Если $r=s$ и $\operatorname{rk}A_i=\operatorname{rk}B_i$ для $i=1,\dots,r$, то говорят, что Σ и Σ' имеют один и тот же ранг.

Следующее утверждение доказывается в точности так же, как и соответствующий факт для разностных векторных пространств (см. теорему 3.11).

Теорема 5.5. *В каждом непустом семействе авторедуцированных множеств дифференциальных многочленов существует множество наименьшего ранга.*

Пусть J — произвольный идеал в кольце $K\{y_1,\dots,y_m\}$. Так как множество всех авторедуцированных подмножеств J непусто (если $A\in J$, то $\{A\}$ — авторедуцированное подмножество J), теорема 5.5 показывает, что идеал J содержит авторедуцированное подмножество наименьшего ранга.

Определение 5.6. Пусть J — идеал в кольце σ-многочленов $K\{y_1,\dots,y_m\}$. Авторедуцированное подмножество в J наименьшего ранга называется характеристическим множеством идеала J.

Следующий результат, полученный в [5] (см. также [14, Theorem 6.4.1]), — разностный аналог классической теоремы Колчина о дифференциальном размерностном многочлене, впервые опубликованной в [11].

Теорема 5.7. *Пусть K — разностное поле с базисным множеством $\sigma=\{\alpha_1,\dots,\alpha_n\}$, T — свободная коммутативная полугруппа, порожденная σ, и для любого $r\in\mathbb{N}$ пусть $T(r)=\{\tau\in T\mid\operatorname{ord}\tau\leqslant r\}$. Пусть, кроме того, $L=K\langle\eta_1,\dots,\eta_m\rangle$ — σ-надполе K, порожденное конечным семейством $\eta=\{\eta_1,\dots,\eta_m\}$. Тогда существует многочлен $\phi_{\eta|K}(t)\in\mathbb{Q}[t]$ со следующими свойствами*:

(i) $\phi_{\eta|K}(r)=\operatorname{trdeg}_K K(\{\tau\eta_j\mid\tau\in T(r),1\leqslant j\leqslant m\})$ *для всех достаточно больших* $r\in\mathbb{N}$;

(ii) $\deg\phi_{\eta|K}(t)\leqslant n$ *и многочлен* $\phi_{\eta|K}(t)$ *можно представить в виде*

$$\phi_{\eta|K}(t)=\sum_{i=0}^{n}a_i\binom{t+i}{i},$$

где $a_0,\dots,a_n\in\mathbb{Z}$;

(iii) *целые числа* a_n, $d=\deg\phi_{\eta|K}(t)$ *и* a_d — *разностные бирациональные инварианты расширения* L/K, *т.е. они не зависят от выбора системы* σ-*порождающих* η. *Кроме того,* $a_n=\sigma\text{-}\operatorname{trdeg}_K L$ *равен разностной степени трансцендентности расширения* L/K $\sigma\text{-}\operatorname{trdeg}_K L$, *т.е. максимальному числу элементов* $\xi_1,\dots,\xi_k\in L$ *таких, что множество* $\{\tau(\xi_j)\mid\tau\in T,1\leqslant j\leqslant k\}$ σ-*алгебраически независимо над* K;

(iv) *пусть* P — *определяющий* σ-*идеал для* $(\eta_1,\dots,\eta_m)$ *в кольце* σ-*многочленов* $K\{y_1,\dots,y_m\}$ *и* $\mathscr{A}$ — *характеристическое множество идеала* P (*в этом случае мы используем последнее определение с* $p=1$). *Кроме того, для всех* $j=1,\dots,m$ *положим*

$$E_j=\{(k_1,\dots,k_n)\in\mathbb{N}^n\mid\alpha_1^{k_1}\dots\alpha_n^{k_n}y_j\text{ — лидер }\sigma\text{-многочлена из }\mathscr{A}\}.$$

Тогда $\phi_{\eta|K}(t)=\sum_{i=1}^{m}\omega_{E_j}(t)$, *где* $\omega_{E_j}(t)$ — *многочлен Колчина множества* E_j.

Многочлен $\phi_{\eta|K}(t)$, существование которого установлено в теореме 5.7, называется *разностным* (или σ-) *размерностным многочленом расширения разностных полей L/K, ассоциированным с системой σ-порождающих η*. Целые числа $d = \deg \phi_{\eta|K}(t)$ и a_d называются, соответственно, *разностным* (или σ-) *типом* и *типовой разностной* (или σ-) *степенью трансцендентности* L над K. Эти разностные бирациональные инварианты L/K обозначаются через $\sigma\text{-type}_K L$ и $\sigma\text{-t.trdeg}_K L$ соответственно. Разностные размерностные многочлены изучались в [1, 6, 14] и др.

В дальнейшем мы используем технику характеристических множеств, ассоциированных с разбиением (1) базисного множества σ, чтобы доказать обобщение последней теоремы и получить новые инварианты конечно порожденных разностных расширений полей. Следующие два утверждения доказываются так же, как теоремы 3.13 и 3.14.

Теорема 5.8. *Пусть $\Sigma = \{A_1, \dots, A_d\}$ — характеристическое множество разностного идеала J кольца разностных многочленов $R = K\{y_1, \dots, y_m\}$. Элемент $B \in R$ редуцирован относительно множества Σ тогда и только тогда, когда $B = 0$.*

Теорема 5.9. *Пусть J — разностный идеал кольца разностных (σ-) многочленов $R = K\{y_1, \dots, y_m\}$, порожденный линейным σ-многочленом f (т.е. f — линейная комбинация элементов TY с коэффициентами из K). Тогда $\{f\}$ — характеристическое множество идеала $J = [f]$.*

Следующая теорема представляет главный результат этого раздела.

Теорема 5.10. *Используя введенные выше обозначения, рассмотрим σ-расширение $L = K\langle \eta_1, \dots, \eta_m \rangle$ поля K, порожденное конечным множеством $\eta = \{\eta_1, \dots, \eta_m\}$. Тогда найдется многочлен $\Phi_\eta(t_1, \dots, t_p)$ от p неизвестных $t_1, \dots, t_p$ с рациональными коэффициентами такой, что справедливы следующие утверждения.*

(i) $\Phi_\eta(r_1, \dots, r_p) = \operatorname{trdeg}_K K\left(\bigcup\limits_{j=1}^{n} T(r_1, \dots, r_p)\eta_j\right)$ *для всех достаточно больших* $(r_1, \dots, r_p) \in \mathbb{N}^p$.

(ii) $\deg_{t_i} \Phi_\eta \leqslant n_i$ $(i = 1, \dots, p)$ *и многочлен Φ_η можно представить в виде*

$$\Phi_\eta(t_1, \dots, t_p) = \sum_{i_1=0}^{n_1} \cdots \sum_{i_p=0}^{n_p} a_{i_1 \dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p},$$

где $a_{i_1 \dots i_p} \in \mathbb{Z}$ для всех $i_1, \dots, i_p$.

(iii) *Пусть $E_\eta = \{(i_1, \dots, i_p) \in \mathbb{N}^p \mid 0 \leqslant i_k \leqslant n_k \ (k = 1, \dots, p)$ и $a_{i_1 \dots i_p} \neq 0\}$. Тогда $d = \deg \Phi_\eta$, $a_{n_1 \dots n_p}$, элементы $(k_1, \dots, k_p) \in E'_\eta$ (мы используем обозначения теоремы 4.6), соответствующие коэффициенты $a_{k_1 \dots k_p}$ и коэффициенты мономов степени d не зависят от выбора системы σ-порождающих η. (Таким образом, эти величины являются разностными бирациональными инвариантами расширения L/K.)*

Доказательство. Пусть P — определяющий идеал σ-расширения полей $K\langle \eta_1, \dots, \eta_m \rangle / K$ и пусть $\Sigma = \{A_1, \dots, A_d\}$ — характеристическое множество идеала P. Если $p > 1$, то для всех $r_1, \dots, r_p \in \mathbb{N}$ положим $U_{r_1 \dots r_p} = \{u \in TY \mid \operatorname{ord}_i u \leqslant r_i$ для $i = 1, \dots, p$ и либо u не является трансформой никакого $u^{(1)}_{A_i}$ (т.е. $u \neq \tau u^{(1)}_{A_i}$ для всех $\tau \in T$; $i = 1, \dots, d$), либо для всех $\tau \in T, A \in \Sigma$, таких что $u = \tau u^{(1)}_A$, найдется $i \in \{2, \dots, p\}$, такое что $\operatorname{ord}_i(\tau u^{(i)}_A) > r_i\}$. Если $p = 1$, положим $U_{r_1} = \{u \in TY \mid \operatorname{ord}_1 u \leqslant r_1$ и u не является трансформой никакого $u^{(1)}_{A_i}\}$. Мы покажем, что множество $\bar{U}_{r_1 \dots r_p} = \{u(\eta) \mid u \in U_{r_1 \dots r_p}\}$ — базис трансцендентности поля $K\left(\bigcup\limits_{j=1}^{n} T(r_1, \dots, r_p)\eta_j\right)$ над K.

Сначала покажем, что множество $\bar{U}_{r_1 \dots r_p}$ алгебраически независимо над K. Пусть g — многочлен от k переменных ($k \in \mathbb{N}$, $k \geqslant 1$) такой, что $g(u_1(\eta), \dots, u_k(\eta)) = 0$ для некоторых элементов $u_1, \dots, u_k \in U_{r_1 \dots r_p}$. Тогда σ-многочлен $\bar{g} = g(u_1, \dots, u_k)$ редуцирован относительно Σ. (В самом

деле, если $p > 1$ и g содержит терм $u = \tau u^{(1)}_{A_i}$ для некоторого i, $1 \leqslant i \leqslant d$, то существует $k \in \{2, \dots, p\}$ такое, что $\operatorname{ord}_k(\tau u^{(j)}_{A_k}) > r_k \geqslant \operatorname{ord}_k u^{(k)}_{\bar g}$). Так как $\bar g \in P$, из теоремы 5.8 вытекает, что $\bar g = 0$. Таким образом, множество $\bar U_{r_1 \dots r_p}$ алгебраически независимо над K.

Теперь мы покажем, что всякий элемент $\tau\eta_j$ ($1 \leqslant j \leqslant m$, $\tau \in T(r_1, \dots, r_p)$) алгебраичен над полем $K(\bar U_{r_1,\dots,r_p})$. Пусть $\tau\eta_j \notin \bar U_{r_1,\dots,r_p}$ (если $\tau\eta_j \in \bar U_{r_1,\dots,r_p}$, то утверждение очевидно). Тогда $\tau y_j \notin U_{r_1,\dots,r_p}$; следовательно, τy_j равен некоторому терму вида $\tau' u^{(1)}_{A_i}$ ($\tau' \in T$, $1 \leqslant i \leqslant d$) такому, что $\operatorname{ord}_k(\tau' u^{(k)}_{A_i}) \leqslant r_k$ для $k = 2, \dots, p$. Представим A_i как многочлен от $u^{(1)}_{A_i}$:

$$A_i = I_0 (u^{(1)}_{A_i})^e + I_1 (u^{(1)}_{A_i})^{e-1} + \dots + I_e,$$

где $I_0, I_1, \dots I_e$ не содержат $u^{(1)}_{A_i}$ (поэтому все термы в этих σ-многочленах младше, чем $u^{(1)}_{A_i}$, относительно порядка $<_1$). Так как $A_i \in P$, имеем

$$A_i(\eta) = I_0(\eta)(u^{(1)}_{A_i})(\eta)^e + I_1(\eta)(u^{(1)}_{A_i})(\eta)^{e-1} + \dots + I_e(\eta) = 0. \tag{6}$$

Легко видеть, что σ-многочлен I_0 редуцирован относительно всех элементов множества Σ. Применяя теорему 5.8, мы получим, что $I_0 \notin P$, откуда $I_0(\eta) \neq 0$. Теперь, если мы применим оператор τ' к обеим частям уравнения (6), полученное уравнение показывает, что элемент $\tau' u^{(1)}_{A_i}(\eta) = \tau\eta_j$ алгебраичен над полем $K(\{\bar\tau\eta_l \mid \operatorname{ord}_i \bar\tau \leqslant r_i$ для $i = 1, \dots, p$; $1 \leqslant l \leqslant m$, и $\bar\tau y_l <_1 \tau' u^{(1)}_{A_i} = \tau y_j\}$. Индукция по множеству термов TY, упорядоченному отношением $<_1$, завершает доказательство факта, что $\bar U_{r_1 \dots r_p}(\eta)$ — базис трансцендентности поля $K\left(\bigcup\limits_{j=1}^{m} T(r_1, \dots, r_p)\eta_j\right)$ над K.

Пусть $U^{(1)}_{r_1 \dots r_p} = \{u \in TY \mid \operatorname{ord}_i u \leqslant r_i$ для $i = 1, \dots, p$ и $u \neq \tau u^{(1)}_{A_j}$ для всех $\tau \in T$; $j = 1, \dots, d\}$ и $U^{(2)}_{r_1 \dots r_p} = \{u \in TY \mid \operatorname{ord}_i u \leqslant r_i$ для $i = 1, \dots, p$ и найдется хотя бы одна пара i, j ($1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant d$) такая, что $u = \tau u^{(1)}_{A_j}$ и $\operatorname{ord}_i(\tau u^{(i)}_{A_j}) > r_i\}$. (Если $p = 1$, положим $U^{(2)}_{r_1 \dots r_p} = \emptyset$). Очевидно, что $U_{r_1 \dots r_p} = U^{(1)}_{r_1 \dots r_p} \cup U^{(2)}_{r_1 \dots r_p}$ и $U^{(1)}_{r_1 \dots r_p} \cap U^{(2)}_{r_1 \dots r_p} = \emptyset$.

Согласно теореме 2.7 существует целозначный многочлен $\omega(t_1, \dots, t_p)$ от p переменных $t_1, \dots, t_p$ такой, что $\omega(r_1, \dots, r_p) = \operatorname{Card} U^{(1)}_{r_1 \dots r_p}$ для всех достаточно больших $(r_1 \dots r_p) \in \mathbb{N}^p$ и $\deg_{t_i} \omega \leqslant n_i$ ($i = 1, \dots, p$). Таким образом, для завершения доказательства теоремы нужно лишь показать, что существует целозначный многочлен $\phi(t_1, \dots, t_p)$ от p переменных $t_1, \dots, t_p$ такой, что $\phi(r_1, \dots, r_p) = \operatorname{Card} U^{(2)}_{r_1 \dots r_p}$ для всех достаточно больших $(r_1 \dots r_p) \in \mathbb{N}^p$ и $\deg_{t_i} \phi \leqslant n_i$ ($i = 1, \dots, p$). Последняя же задача была фактически решена в доказательстве теоремы 4.2. Действуя как и в том доказательстве, мы получаем желаемый многочлен $\phi(t_1, \dots, t_p)$ как альтернированную сумму многочленов вида (5), степени которых по каждой переменной t_i не превосходят n_i ($1 \leqslant i \leqslant p$). Это завершает доказательство первых двух утверждений теоремы.

Пусть $\zeta = \{\zeta_1, \dots, \zeta_q\}$ — другая система σ-порождающих расширение L/K и пусть

$$\Phi_\zeta(t_1, \dots, t_p) = \sum_{i_1=0}^{n_1} \dots \sum_{i_p=0}^{n_p} b_{i_1 \dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p}$$

— размерностный многочлен этого расширения, ассоциированный с системой порождающих ζ. Тогда существуют натуральные числа $s_1, \dots, s_p$, такие что

$$\eta_i \in K\left(\bigcup_{j=1}^{q} T(s_1, \dots, s_p)\zeta_j\right), \quad \zeta_k \in K\left(\bigcup_{j=1}^{m} T(s_1, \dots, s_p)\eta_j\right)$$

для всех $i = 1, \dots, m$ и $k = 1, \dots, q$. Поэтому

$$\Phi_\eta(r_1, \dots, r_p) \leqslant \Phi_\zeta(r_1 + s_1, \dots, r_p + s_p), \quad \Phi_\zeta(r_1, \dots, r_p) \leqslant \Phi_\eta(r_1 + s_1, \dots, r_p + s_p)$$

для всех достаточно больших $(r_1, \dots, r_p) \in \mathbb{N}^p$. Эти два неравенства сразу влекут последнее утверждение теоремы. □

Многочлен $\Phi_\eta(t_1, \dots, t_p)$, существование которого установлено теоремой 5.10, называется $(\sigma_1, \dots, \sigma_p)$-*размерностным многочленом* разностного (σ-) расширения полей L/K, ассоциированного с множеством разностных порождающих $\eta = \{\eta_1, \dots, \eta_m\}$ (и разбиением $\sigma = \sigma_1 \cup \dots \cup \sigma_p$ базисного множества σ).

Следующий пример показывает, что если $p > 1$, то $\Phi_\eta(t_1, \dots, t_p)$ содержит существенно больше разностных бирациональных инвариантов L/K, чем разностный размерностный многочлен от одной переменной, определенный в теореме 5.7.

Пример 5.11. Пусть K — разностное поле с базисным множеством $\sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ и пусть $\sigma_1 = \{\alpha_1\}$, $\sigma_2 = \{\alpha_2\}$, $\sigma_3 = \{\alpha_3\}$, так что мы зафиксировали разбиение $\sigma = \sigma_1 \cup \sigma_2 \cup \sigma_3$ базисного множества σ. Кроме того, пусть L — σ-расширение поля L, порожденное одним элементом η (так что $L = K\langle\eta\rangle$) с определяющим уравнением

$$\alpha_1^{a+c}\alpha_2^b\eta + \alpha_2^{a+b}\alpha_3^c\eta + \alpha_1^a\alpha_3^{b+c}\eta = 0,$$

где a, b и c — натуральные числа. (Это значит, что определяющий σ-идеал η над K — σ-идеал кольца σ-многочленов $K\{y\}$, порожденный $f = \alpha_1^{a+c}\alpha_2^b y + \alpha_2^{a+b}\alpha_3^c y + \alpha_1^a\alpha_3^{b+c}y$. Так как σ-многочлен f линеен, идеал $[f]$ прост, см. [14, Proposition 3.2.28].)

Пусть $\Phi_\eta(t_1, t_2, t_3)$ и $\phi_\eta(t)$ — $(\sigma_1, \sigma_2, \sigma_3)$-размерностный и σ-размерностный многочлены L/K, ассоциированные с σ-образующей η. Как и в доказательстве теоремы 5.10, получаем

$$\begin{aligned}\Phi_\eta(t_1, t_2, t_3) = &\left[\binom{t_1+1}{1}\binom{t_2+1}{1}\binom{t_3+1}{1} - \binom{t_1+1-(a+c)}{1}\binom{t_2+1-b}{1}\binom{t_3+1}{1}\right] + \\ &+ \Big[\big(t_1-(a+c)+1\big)a(t_3+1) + \big(t_1-(a+c)+1\big)(t_2-b+1)(b+c) - \\ &- \big(t_1-(a+c)+1\big)a(b+c)\Big] = \\ &= (b+c)t_1t_2 + (a+b)t_1t_3 + (a+c)t_2t_3 + \text{термы степени} < 2,\end{aligned}$$

и

$$\phi_\eta(t) = \binom{t+3}{3} - \binom{t+3-(a+b+c)}{3} = \frac{a+b+c}{2}t^2 + \text{термы степени} < 2.$$

Теоремы 5.7 и 5.10 показывают, что многочлен $\phi_\eta(t)$ содержит лишь разностный бирациональный инвариант $a+b+c$, тогда как $\Phi_\eta(t_1, t_2, t_3)$ определяет три инварианта $a+b$, $a+c$ и $b+c$, т.е. Φ_η определяет все три параметра определяющего уравнения, в то время как $\phi_\eta(t)$ дает лишь сумму этих параметров.

СПИСОК ЛИТЕРАТУРЫ

1. *Балаба И. Н.* Размерностные многочлены расширений разностных полей// Вестн. МГУ. Сер. мат. мех. — 1984. — *2*. — С. 31–35.
2. *Кондратьева М. В., Панкратьев Е. В., Серов Р. Е.* Вычисления в дифференциальных и разностных модулях// В кн.: «Аналитические вычисления на ЭВМ и их применение в теоретической физике»/ ДП-85-791. — ОИЯИ, 1985. — С. 208–213.
3. *Латышев В. Н.* Комбинаторная теория колец. Сложность алгебраических алгоритмов. — М.: МГУ, 1987.
4. *Латышев В. Н.* Комбинаторная теория колец. Стандартные базисы. — М.: МГУ, 1988.
5. *Левин А. Б.* Характеристические многочлены фильтрованных разностных модулей и расширений разностных полей// Усп. мат. наук. — 1978. — *33*, № 3. — С. 165–166.
6. *Левин А. Б., Михалев А. В.* Размерностные многочлены дифференциально-разностных модулей и расширений дифференциально-разностных полей// Абелевы группы и модули. — 1991. — *10*. — С. 56–82.
7. *Михалев А. В., Панкратьев Е. В.* Дифференциальный размерностный многочлен системы дифференциальных уравнений// В кн.: «Алгебра»/ Сб. под ред. А. И. Кострикина. — М.: МГУ, 1980. — С. 57–67.

8. *Михалев А. В., Панкратьев Е. В.* Компьютерная алгебра. Вычисления в дифференциальной и разностной алгебре. — М.: МГУ, 1989.
9. *Cohn R. M.* Difference algebra. — N.Y.: Interscience, 1965.
10. *Johnson J.* Differential dimension polynomials and a fundamental theorem on differential modules// Amer. J. Math. — 1969. — *91*. — С. 239–248.
11. *Kolchin E. R.* The notion of dimension in the theory of algebraic differential equations// Bull. Amer. Math. Soc. — 1964. — *70*. — С. 570–573.
12. *Kolchin E. R.* Differential algebra and algebraic groups. — N.Y.: Academic Press, 1973.
13. *Kondrat'eva M. V., Levin A. B., Mikhalev A. V., Pankrat'ev E. V.* Computation of dimension polynomials// Int. J. Algebra Comput. — 1992. — *2*. — С. 117–137.
14. *Kondrat'eva M. V., Levin A. B., Mikhalev A. V., Pankrat'ev E. V.* Differential and difference dimension polynomials. — Dordrecht: Kluwer Acad. Publ., 1998.
15. *Latyshev V. N.* General version of standard bases in linear structures// In: *Algebra*/ Moscow, 1998. — Berlin: de Gruyter, 2000. — С. 215–226.
16. *Latyshev V. N.* An improved version of standard bases// In: «Formal Power Series and Algebraic Combinatorics». — Berlin: Springer-Verlag, 2000. — С. 496–505.
17. *Levin A. B.* Reduced Gröbner bases, free difference-differential modules, and difference-differential dimension polynomials// J. Symbol. Comput. — 2000. — *29*. — С. 1–26.
18. *Pankrat'ev E. V.* Computations in differential and difference modules// Acta Appl. Math. — 1989. — *16*, № 2. — С. 167–189.

А. Б. Левин
Department of Mathematics, The Catholic University of America, Washington, D. C. 20064
E-mail: levin@cua.edu

Современная математика и ее приложения. Том 14 (2004). С. 71–85

УДК 512.55

О ЛОКАЛЬНО КОНЕЧНЫХ МОДУЛЯХ

© 2004 г. **А. МЕКЕЙ, Р. ВИСБАУЭР**

Аннотация. Статья посвящена изучению *локально конечных модулей* M, т.е. модулей, конечно порожденные подмодули которых конечны (как множества). В частности, изучаются кольца с точными локально конечными модулями, например, кольца многочленов $\mathbb{Z}[x]$ и $F[x]$, где F — конечное поле. Полученные результаты обобщают свойства абелевых групп с кручением и кольца целых чисел.

СОДЕРЖАНИЕ

1. Введение

Различные типы условий локальной конечности модулей можно рассматривать, например, для локально нетеровых модулей, локально артиновых модулей, модулей локально конечной длины и остаточно конечных модулей. В этой статье рассматривается более сильное условие локальной конечности в категории модулейю Пусть A — произвольное ассоциативное кольцо с единицей.

Определение 1.1. Правый A-модуль M называется *локально конечным*, если любой конечно порожденный подмодуль модуля M конечен (как множество). Кольцо A называется *локально конечным справа*, если существует точный правый локально конечный A-модуль. Кольцо A (модуль M) называется *остаточно конечным*, если A (соответственно M) — подпрямое произведение конечных колец (модулей).

В разделе 2 рассматриваются общие свойства локально конечных модулей. В разделах 3 и 4 изучаются соответственно локально конечные $GF(p^n)[x]$-модули и локально конечные $\mathbb{Z}[x]$-модули и даются различные характеризации этих модулей.

Введем некоторые обозначения. Пусть $J(A)$ — радикал Джекобсона кольца A. Если B — подкольцо A, то $[A : B]$ — индекс абелевой группы $(B, +)$ в $(A, +)$, т.е. мощность смежных классов. Обозначения $B \hookrightarrow A$ и d $N \hookrightarrow M$ означают, что B — подкольцо кольца A, а N — подмодуль модуля M. Обозначение $[A : B] < \infty$ означает, что B имеет конечный индекс в A.

Единицей кольца A называется многочлен $f(x_1, \ldots, x_n)$ от некоммутативных переменных $X = \{x_1, \ldots x_n\}$ таких, что $f(a_1, \ldots, a_n) = 0$ для любого $a_1, a_2, \ldots, a_n \in A$. *Многообразием ассоциативных колец* $\mathscr{M}$ называется (непустой) класс колец, определяемых некоторой системой тождеств.

Пусть $f \in \mathbb{Z}[x]$. Старший коэффициент f обозначается через $a_0(f)$, а идеал, порожденный f, — через (f). Обозначение $A = \prod_{i \in I}^{s} A_i$ означает, что кольцо A есть подпрямое произведение колец A_i, $i \in I$.

ISSN 1512–1712

2. Общие свойства локально конечных A-модулей

Ясно, что подмодули, гомоморфные образы и прямые суммы локально конечных A-модулей являются локально конечными A-модулями. Следовательно, класс локально конечных A-модулей образует полную категорию A-модулей, замкнутую относительно этих операций. Эта категория является подкатегорией типа $\sigma[M]$, подпорожденной некоторым подходящим A-модулем M (см. [6]). Примеры строгих локально конечных A-модулей:

1) $A = \mathbb{Z}$, $M = \mathbb{Z}_{p\in ty}$, p — простое число (прюферовы группы);
2) $A = GF(p^n)$ — конечное поле, M — произвольное векторное пространство над A;
3) A — конечное кольцо, M — произвольный точный A-модуль.

Напомним некоторые очевидные свойства локально конечных A-модулей. Для бесконечного кольца A строгие локально конечные A-модули не могут быть конечно порожденными. Абелева группа M может быть локально конечным A-модулем для некоторого кольца A, но не локально конечным модулем для некоторого другого кольца. Например, бесконечномерное векторное пространство V над конечным полем локально конечно как $GF(p^n)$-модуль, но не локально конечно как $\mathrm{End}_{GF(p)}(V)$-модуль.

Теорема 2.1. *Кольцо A допускает точный локально конечный правый A-модуль (локально конечный A-модуль) в том и только том случае, если A — остаточно конечное (аппроксимируемое конечными кольцами) кольцо.*

Доказательство. Пусть M — точный локально конечный A-модуль. Тогда для любого $m \in M$ подмодуль mA конечен. Аннулятор $\mathrm{An}(m) = \{r \in A \mid mr = 0\}$ в A имеет конечный индекс в A. Подмодуль mA изоморфен конечному A-модулю $(A/\mathrm{An}(m), +)$. Легко доказывается (см., например, [2]), что правый идеал $\mathrm{An}(m)$ содержит идеал конечного индекса в A. Обозначая этот идеал через $B(m)$, получаем, что $A/B(m)$ — конечное кольцо. Так как M — точный A-модуль, то $\bigcap\limits_{m\in M} B(m) = (0)$. Это означает, что A — остаточно конечное кольцо.

Пусть теперь кольцо A остаточно конечно, т.е. $A = \prod\limits_{I}^{s} A_i$, где A_i — конечные кольца, а естественное отображение $\pi_i : A = \prod\limits_{I}^{s} A_i \to A_i$ — эпиморфизм для любого $i \in I$. Это дает семейство идеалов $I_i = \ker \pi_i$ и абелевы группы $M_i = (A/I_i, +)$, $i \in I$. Ясно, что любой M_i есть конечный правый A-модуль и прямая сумма $M = \bigoplus\limits_{i\in I} M_i$ есть точный правый A-модуль, а также и локально конечный A-модуль. Это и доказывает теорему. □

Следствие 2.2. *Кольца $\mathbb{Z}$, $\mathbb{Z}[x]$, $GF(p^k)[x]$, а также все конечные кольца с единицей доускают правые локально конечные модули.*

Доказательство. Хорошо известно, что все эти кольца остаточно конечны. □

Следствие 2.3. *Пусть R — остаточно конечное кольцо, а G — остаточно конечная группа. Тогда групповое кольцо $R[G]$ допускает точный локально конечный модуль.*

Доказательство. Групповое кольцо $R[G]$ остаточно конечно (см. [5]). □

Следствие 2.4. *Пусть $\mathscr{M}$ — многообразие ассоциативных колец, удовлетворяющих тождествам вида*

$$p^2 x = 0, \qquad xy = f(x, y), \tag{2.1}$$

где p — простое число, $\deg f(x, y) \geqslant 3$. Тогда любое кольцо с единичным элементом $\mathscr{M}$ допускает точный локально конечный модуль.

Доказательство. В [4] доказано, что $\mathscr{M}$ есть многообразие аппроксимируемых колец в том и только том случае, если $\mathscr{M}$ удовлетворяет тождествам вида (2.1). Наше утверждение следует из теоремы 2.1. □

Предложение 2.5. *Пусть A — локальное кольцо. Кольцо A допускает точный локально конечный модуль в том и только том случае, если $A/J(A)$ — конечное поле, а $J(A)$ аппроксимируемо конечными нильпотентными кольцами.*

Доказательство. Пусть A допускает локально конечный модуль M. Тогда для любого $m \in M$ подмодуль mA конечен и потому A-модуль $m(A/J(A))$ также конечен. Предположим, что $m(A/J(A)) \neq 0$. Поскольку $A/J(A)$ — тело, то отсюда следует, что $A/J(A)$ — конечное поле. Кроме того, $mJ(A)$ — конечный A-модуль. Следовательно, $\mathrm{An}_J(m) = \{x \in J(A) \mid mx = 0\}$ — правый идеал в A. Ясно, что $J(A)/\mathrm{An}_J(m)$ также конечен; отсюда следует, что индекс $[A : \mathrm{An}_J(m)]$ конечен. Тогда $\mathrm{An}_J(m)$ содержит идеал A_i в A такой, что $[A : A_i] < \infty$ (см. [2]). Когда m пробегает все элементы M, семейство идеалов $\{A_i, i \in I\}$, где I — множество индексов, зависящее от M, имеет нетривиальное пересечение $\bigcap\limits_I A_i = (0)$, поскольку M — точный A-модуль. Так как $A_i \hookrightarrow J(A)$, получаем, что $J(A)/A_i$ — конечные радикальные кольца и, следовательно, они конечны и нильпотентны, а потому $J(A)$ конечно аппроксимируемо конечными нильпотентными кольцами.

Обратно, пусть $J(A) = \prod\limits_{i\in I}^{s} J_i$, где все J_i — конечные кольца, и пусть $\pi_i : J(A) = \prod\limits_{i\in I}^{s} J_i \to J_i$ — естественные проекции. Тогда имеем семейство идеалов $\{A_i = \ker \pi_i, i \in I\}$ в $J(A)$, каждый из которых имеет конечный индекс в $J(A)$. Поэтому $[A : J(A)]$ и $[J(A) : A_i]$ конечны и, следовательно, индекс $[A : A_i]$ конечен. Тогда A_i содержит идеал B_i конечного индекса в A (см. [2, Lemma 1]). Теперь из равенства $0 = \bigcap A_i \supseteq \bigcap B_i$ следует, что A — конечно аппроксимируемое кольцо. Согласно теореме 2.1 A допускает точный локально конечный модуль. □

Следствие 2.6. *Кольцо степенных рядов $GF(p^n)[[x]]$ допускает точный локально конечный модуль.*

Предложение 2.7. *Артиново кольцо A допускает точный локально конечный модуль в том и только том случае, если A удовлетворяет тождествам вида*

$$x^n + x^{n+1} f = 0, \tag{2.2}$$

где $f \in \mathbb{Z}[x]$, а радикал $J(A)$ кольца A аппроксимируем конечными нильпотентными кольцами.

Доказательство. Пусть M — локально конечный A-модуль. Тогда для любого $m \in M$ модули mA и $m(A/J(A))$ конечны. Как известно, $A/J(A)$ — конечная прямая сумма матричных колец над телами. Пусть

$$A/J(A) = \Delta_{m_1}^{(1)} \oplus \cdots \oplus \Delta_{m_k}^{(k)},$$

где $m_i \geqslant 1$, $i = 1, 2, \ldots, k$, а $\Delta^{(i)}$, $i = 1, 2, \ldots, k$, — тела. Тогда $m\Delta_{m_i}^{(i)}$ также конечно. Отсюда следует, что $m\Delta^{(i)}$ конечно при всех $i = 1, 2, \ldots, k$; значит $\Delta^{(i)}$ конечно. Это означает, что кольцо $\bar{A} = A/J(A)$ — конечное кольцо и (см. [1]) $\bar{A}$ удовлетворяет тождеству вида $x^k - x^s = 0$, где $k > s \geqslant 1$. Кольцо A артиново, а $J(A)$ нильпотентно, поэтому A удовлетворяет тождеству $(x^k x^s)^r = 0$, где $J(A)^r = 0$. Тождество $(x^k - x^s)^r = 0$ имеет вид $x^{sr} + x^{sr+1} f = 0$. Из неравенства $|mA| < \infty$ следует, что $mJ(A)$ также конечно. Пусть

$$\mathrm{An}_J(m) = \{x \in J(A) \mid mx = 0\};$$

$\mathrm{An}_J(m)$ — правый идеал в A, имеющий конечный индекс в $J(A)$. Тогда из неравенств $[A : J(A)] < \infty$ и $[J(A) : \mathrm{An}_J(m)] < \infty$ следует, что $\mathrm{An}_J(m)$ имеет конечный индекс в A, $[A : \mathrm{An}_J(m)] < \infty$. Тогда $\mathrm{An}_J(m)$ содержит идеал в A конечного индекса (см. [2, лемма 1]). Обозначим этот идеал через I_i, где $I_i \subseteq \mathrm{An}_J(m)$; тогда $[A : I_i] < \infty$. Так как M — точный A-модуль, то $\bigcap\limits_{i\in I} I_i = (0)$. Следовательно,

$$J(A) = \prod\nolimits^{s} J(A)/I_i := \prod_{m\in I}^{s} J_i,$$

где $J_i = J(A)/I_i$. Пусть теперь A удовлетворяет заданным условиям. Из тождества (2.2) следует, что $A/J(A)$ — конечное кольцо. Естественные проекции $\pi_i : J(A) = \prod_{i\in I}^{s} J_i \to J_i$ дают семейство идеалов $\ker \pi_i = I_i \lhd J(A)$ конечного индекса и $\bigcap_{i\in I} I_i = (0)$. Группы $A/J(A)$ и $J(A)/I_i$ — конечные абелевы группы. Отсюда следует, что A/I_i конечно при всех $i \in I$. Тогда I_i содержит идеал $A_i \lhd A$, а $A_i \subseteq I_i$ также имеет конечный индекс в A (см. [2, лемма 1]). Поэтому получаем семейство идеалов $\{A_i, i \in I\}$ кольца A такое, что $\bigcap A_i = 0$ и $[A : A_i]$ конечен. Следовательно, A аппроксимируемо конечными кольцами. Тогда по теореме 2.1, A допускает точный локально конечный модуль. □

Полная подкатегория всех локально конечных модулей в A-Mod имеет вид $\sigma[M]$, где M — некоторый A-модуль, который можно считать образующей этой подкатегории. Опишем те модули M, которые являются образующими или подобразующими в этой категории. Ясно, что любой правый локально конечный модуль порожден конечными модулями типа A/I для некоторого правого идеала $I \subset A$ и I содержит двусторонний идеал $K \subset I$ такой, что A/K конечен (см. [2, лемма 1]). Это доказывает следующую теорему.

Теорема 2.8. *Подкатегория локально конечных модулей в* A-Mod *порождена* A*-модулем*

$$M(A) = \bigoplus \{A/K \mid K \subset A - \textit{идеал с конечным } A/K\}.$$

Следствие 2.9. (i) *Подкатегория локально конечных модулей в* $\mathbb{Z}$-Mod *порождена* $\mathbb{Z}$*-модулем*

$$M(\mathbb{Z}) = \bigoplus_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$$

и совпадает с подкатегорией модулей с кручением в $\mathbb{Z}$-Mod.

(ii) *Для кольца степенных рядов* $A = GF(p^n)[[x]]$ *подкатегория локально конечных модулей в* A-Mod *порождена* A*-модулем*

$$M(A) = \bigoplus_{k=1}^{\infty} A/x^k A.$$

(iii) *Для кольца многочленов* $R = GF(p^n)[x]$ *подкатегория локально конечных модулей в категории* R-Mod *порождена* R*-модулями*

$$M(R) = \bigoplus_{h} \bigoplus_{k=1}^{\infty} V_k(h) \quad \textit{или} \quad M(R) = \bigoplus_{s=1}^{\infty} \bigoplus_{f} \bigoplus_{n=1}^{\infty} V_n(f^s),$$

где $h \in R$, $k = \deg h$, *или* f *— неприводимый многочлен,* $n = \deg f$, $s \geqslant 1$, *а* $V_k(h) = (R/hR, +)$ *и* $V_n(f^s) = (R/f^sR, +)$ *—* R*-модули.*

Доказательство. (i) Любой идеал в $\mathbb{Z}$ имеет вид $n\mathbb{Z}$. Следовательно, ввиду коммутативности $\mathbb{Z}$, в теореме 2.8 имеем $K = n\mathbb{Z}$.

(ii) Кольцо $A = GF(p^n)[[x]]$ является также и областью главных идеалов; любой идеал I в A имеет вид $I = x^k A$. Поэтому любой конечно порожденный A-модуль изоморфен A-модулю типа $A/x^k A$ или гомоморфному образу прямой суммы A-модулей этого типа. Следовательно, локально конечные модули порождаются прямой суммой $\bigoplus_{k=1}^{\infty} A/x^k A$.

(iii) Кольцо $R = GF(p^n)[x]$ есть область главных идеалов, поэтому любой идеал I в R имеет вид $I = hR$ для некоторого $h \in R$. Тогда любой конечно порожденный локально конечный модуль изоморфен суммам R-модулей типа $(R/hR, +)$. Обозначим $V_k(h) = R/hR$, где $k = \deg h$. В случае, когда h — неприводимый многочлен и $h = f_1^{s_1} \cdots f_m^{s_m}$ — разложение h в произведение неприводимых

многочленов f_i, $i = 1, \ldots, m$, хорошо известно, что

$$R/hR \simeq \bigoplus_{i=1}^{m} R/f_i^{s_i}R = \bigoplus_{i=1}^{m} V_{n_i}(f^{s_i}),$$

где $V_{n_i}(f_i^{s_i}) = (R/f_i^{s_i}R, +)$ и $n_i = \deg f_i$. Из этих рассмотрений видно, что локально конечные модули порождены R-модулями

$$\bigoplus_{k=1}^{\infty}\bigoplus_{h} V_k(h) \quad \text{или} \quad \bigoplus_{s=1}^{\infty}\bigoplus_{n_f=1}^{\infty}\bigoplus_{f} V_{n_f}(f^s),$$

где $1 \leqslant k, s, n$ — числа, h и f — многочлены, $\deg h = k$, $\deg f = n_f$, а многочлен f неприводим. □

3. Категория локально конечных $GF(p^n)[x]$-модулей

Положим снова $R = GF(p^n)[x]$. Заметим, что в конце предыдущего раздела было показано, что любой конечно порожденный подмодуль локально конечного R-модуля изоморфен прямой сумме R-модулей типа $V_k(f^s)$, где $k = \deg f$, f — неприводимый многочлен, а $s \geqslant 1$. Это рассуждение сводит исследование R-модулей в подкатегории локально конечных модулей к исследованию локально конечных R-модулей типа $V_k(f^s)$. R-модуль $V_k(f^s)$, рассматриваемый как $GF(p^n)$-пространство, обладает базисом 1, x, x^2, …, x^{k-1}, …, x^{ks-1}. Согласно алгоритму Евклида, запишем $x^k, \ldots, x^{ks-1}$ как степени f типа

$$x^{k+m} = x^m f + a_1 x^{m-1} f + \cdots + a_m f + \varphi_1, \tag{3.1}$$

где $\deg \varphi_1 \leqslant k - 1$. Из (3.1) получаем доказательство следующей леммы.

Лемма 3.1. *Локально конечный R-модуль $V_k(f^s)$, рассматриваемый как $GF(p^n)$-векторное пространство, допускает базис*

$$1,\ x,\ \ldots,\ xk-1,\ f,\ xf,\ \ldots,\ x^{k-1}f,\ \ldots,\ f^{s-1},\ xf^{s-1},\ \ldots,\ x^{k-1}f^{s-1}. \tag{3.2}$$

Рассмотрим последовательность R-модулей

$$V_k(f),\ V_k(f^2),\ \ldots,\ V_k(f^s),\ \ldots \tag{3.3}$$

и установим связь между ними. Из леммы 3.1 следует, что если умножить на f все порождающие элементы $V_k(f^s)$, то получим последовательность элементов без 1, x, …,x^{k-1} из (3.2). Базис $GF(p^n)$-пространства $V_k(f^{s-1})$ состоит из элементов (3.2) без последних k элементов f^{s-1}, xf^{s-1}, …, $x^{k-1}f^{s-1}$. Можно определить линейное отображение

$$\pi_f : V_k(f^{s-1}) \to V_k(f^s), \quad \varphi \mapsto f \cdot \varphi. \tag{3.4}$$

Поскольку для любого $g \in R$ имеем $\varphi \circ g = \varphi \cdot g (\mathrm{mod}\, f^{s-1})$ в $V_k(f^{s-1})$, а

$$\pi_f(\varphi \circ g) = \pi_f(\varphi \cdot g(\mathrm{mod}\, f^{s-1})) = f \cdot (\varphi \cdot g(\mathrm{mod}\, f^s)) = (f\varphi) \cdot g(\mathrm{mod}\, f^s) = f\varphi \circ g = \pi_f(\varphi) \circ g$$

в $V_k(f^s)$, то это показывает, что (3.4) есть морфизм R-модулей. Очевидно, что π_f есть мономорфизм; это дает, что $V_k(f^{s-1})$ изоморфен подмодулю $f(V_k(f^s))$ в $V_k(f^s)$, а потому

$$V_k(f^{s-1}) \cong fV_k(f^s). \tag{3.5}$$

Из (3.5) следует, что

$$\begin{gathered} V_k(f) \cong fV_k(f^2) \cong f^2V_k(f^3) \cong \cdots \cong f^{s-1}V_k(f^s), \\ V_k(f^2) \cong fV_k(f3) \cong \cdots \cong f^{s-2}V_k(f^s) \subseteq V_k(f^3) \cong fV_k(f^4) \cong \cdots \cong f^{s-3}V_k(f^s) \cong \cdots . \end{gathered} \tag{3.6}$$

После отождествления изоморфных модулей в (3.6) получаем возрастающую цепь локально конечных модулей

$$V_k(f) \subset V_k(f^2) \subset V_k(f^3) \subset \cdots \subset V_k(f^s) \subset \cdots . \tag{3.7}$$

Введем обозначение

$$V_k(f^\infty) = \bigcup_{s=1}^{\infty} V_k(f^s).$$

Заметим, что, используя изоморфизм (3.6), можно рассмотреть прямые суммы и найти их прямой предел обычным образом; покажем, что этот прямой предел состоит из $V_k(f^\infty)$. Из (3.7) следует, что любой элемент a из $V_k(f^\infty)$ имеет вид

$$a = \varphi_1 f^r + \varphi_2 f^{r+1} + \cdots + \varphi_m f^{r+m}, \tag{3.8}$$

где φ_i — многочлен такой, что $\deg \varphi_i \leqslant k-1$, $1 \leqslant r \in \mathbb{N}$.

Лемма 3.2. *Следующие утверждения справедливы для R-модуля $V_k(f^\infty)$:*

(i) любой собственный подмодуль $V_k(f^\infty)$ конечен;
(ii) любая убывающая цепь подмодулей в $V_k(f^\infty)$ становится устойчивой после конечного числа шагов;
(iii) любой гомоморфный образ $V_k(f^\infty)$ изоморфен самому себе;
(iv) R-модуль $V_k(f^\infty)$ порожден бесконечным множеством линейно независимых над $GF(p^n)$ элементов.

Доказательство. (i) Пусть M — собственный R-подмодуль $V_k(f^\infty)$. Заметим, что $V_k(f^s)$ также является и кольцом. Ясно, что в силу (3.8) любой элемент M имеет вид (3.8) и его можно представить в виде

$$a = f^r(\varphi_1 + \varphi_2 f^2 + \cdots + \varphi_m f^m), \quad a \in V_k(f^s),$$

для некоторых $s \geqslant 1$ и $\varphi_1 \neq 0$, $\deg \varphi_1 \leqslant k-1$. Тогда многочлен $\varphi = \varphi_1 + \varphi_2 f^2 + \cdots + \varphi_m f^m$ обратим $\mathrm{mod}(f^s)$, поскольку $\varphi_1 \neq 0$. Следовательно, для некоторого $u \in R$, имеем $a \cdot u = f^r (\mathrm{mod}\, f^s)$. Если $f^r \in M$ для всех $= 1, 2, \ldots, r, r+1, \ldots$, то M совпадает с $V_k(p^\infty)$; это противоречит тому, что M — собственный подмодуль $V_k(f^\infty)$. Значит, существуют $m \geqslant 1$ такие, что $f^m \in M$ $f^{m+1} \notin M$. Отсюда следует, что M конечен.

(ii) тривиально следует из (i).

(iii) Легко видеть, что

$$V_k(f^s)/V_k(f^m) \cong V_k(f^s)/f^{s-m}V_k(f^s) \cong V_k(f^{s-m}).$$

Пусть M — ядро гомоморфизма модуля $V(f^\infty)$. Тогда M изоморфен подмодулю типа $V_k(f^m)$, …, $V_k(f)$. Из (3.7) следует, что $V_k(f^\infty)$ изоморфен любому своему гомоморфному образу.

(iv) следует из (i). В самом деле, пусть любое бесконечное множество элементов $V_k(f^\infty)$, линейно независимых над полем $GF(p^n)$, порождает собственный подмодуль в $V_k(f^\infty)$. Тогда этот подмодуль конечен в силу (i); следовательно, он не допускает бесконечного множества линейно независимых элементов. □

Теорема 3.3. *Пусть $R = GF(p^n)[x]$ и пусть $Q(R)$ — факторполе R. Тогда выполняются следующие утверждения в подкатегории локально конечных модулей в R-*Mod:

(i) *$Q(R)/R$ — инъективный локально конечный модуль*;
(ii) *$V_k(f^\infty)$ инъективен для всех неприводимых многочленов f и является инъективной оболочкой простых R-модулей $V_k(f)$, где $k = \deg f$*;
(iii) *$Q(R)/R$ есть кообразующая этой подкатегории, а сама подкатегория не является конечно порожденной*;
(iv) *$V_k(f^\infty)$ есть когенератор подкатегории*

$$\sigma[V_k(f^\infty)] = \sigma\left[\bigoplus_{s=1}^{\infty}\bigoplus_{k=1}^{\infty} V_k(f^s)\right],$$

где f — неприводимый многочлен.

Доказательство. Так как $R = GF(p^n)[x]$ — область главных идеалов, то $Q(R)$ инъективен как R-модуль; отсюда следует, что $\overline{Q(R)} := Q(R)/R$ инъективен. Кроме того, $\overline{Q(R)}$ — локально конечный R-модуль. Пусть f — неприводимый многочлен. Обозначим через $V_k\left(\frac{1}{f^\infty}\right)$ все дроби со знаменателями — степенями f; тогда любой элемент z из $V_k\left(\frac{1}{f^\infty}\right)$ имеет вид

$$z = \frac{\varphi_1}{f} + \frac{\varphi_2}{f^2} + \cdots + \frac{\varphi_m}{f^m},$$

где $\deg \varphi_i < \deg f = k$, $m \geqslant 1$ (φ_i может быть постоянным многочленом). Следовательно, обычное разложение рациональных дробей показывает, что

$$\overline{Q(R)} = \bigoplus_k \bigoplus_f V_k\left(\frac{1}{f^\infty}\right).$$

Установим теперь R-модульный изоморфизм между $V_k(f^\infty)$ и ${}_k\left(\frac{1}{f^\infty}\right)$. Определим R-линейное отображение $\varphi : V_k(f^\infty) \to V_k\left(\frac{1}{f^\infty}\right)$ по правилу

$$h = \varphi_0 + \varphi_1 f + \varphi_2 f^2 + \cdots + \varphi_m f^m \mapsto \frac{\varphi_0}{f^{m+1}} + \frac{\varphi_1}{f^m} + \cdots + \frac{\varphi_m}{f} = \varphi(h), \tag{3.9}$$

поскольку $h \in V_k(f^{m+1})$ и h имеет порядок $f^{m+1} (\mathrm{mod}\, f^{m+1})$, а $\varphi(h)$ также имеет порядок f^{m+1}, $f^{m+1} \cdot \varphi(h) \equiv 0 (\mathrm{mod}\, R)$. Следовательно,

$$V_k(f^\infty) \cong V_k\left(\frac{1}{f^\infty}\right), \quad \overline{Q(R)} \cong \bigoplus_{k=1}^{\infty} \bigoplus_f V_k(f^\infty).$$

$V_k(f^\infty)$ инъективен как прямое слагаемое в инъективном модуле и также содержит простой R-модуль $V_k(f)$; на самом деле он является его инъективной оболочкой. Из этих рассмотрений вытекают все утверждения теоремы. □

4. Категория локально конечных $\mathbb{Z}[x]$-модулей

Пусть $A = \mathbb{Z}[x]$ — кольцо многочленов с целыми коэффициентами. Рассмотрим далее идеалы типа $H(p^n, h)$, порожденные p^n и h в $\mathbb{Z}[x]$, где p — простое число, а h — многочлен с целыми коэффициентами, $n \geqslant 1$. Предположим, что все коэффициенты h меньше, чем p^n. В этом случае факторкольцо $\mathbb{Z}[x]/H(p^n, h)$ изоморфно кольцу $(\mathbb{Z}/p^n\mathbb{Z})[x]/(h)$. Если старший коэффициент $a_0(h)$ многочлена h относительно прост с p^n, то рассмотрим h как исходный многочлен. Пусть $(a_0(h), p^n) = p^k$, $1 \leqslant k < n$, и пусть h регулярен (не является делителем нуля). Тогда (см. [3]) h допускает представление $h = (1 + g)h^\star$ в $(\mathbb{Z}/p^n\mathbb{Z})[x]$, где $\deg h^\star \leqslant \deg h$, $1 + g$ обратим, $h^\star$ — унитальный многочлен и $(h) = (h^\star)$. Идеалы типа $H(p^n, p^k h)$, где $1 \leqslant k < n$ и h примитивны, не будут рассматриваться здесь, поскольку в этом случае $p^k h$ не регулярен в кольце $(\mathbb{Z}/p^n\mathbb{Z})[x]$ и факторкольцо $(\mathbb{Z}/p^n\mathbb{Z})[x]/(pkh)$ не конечно. Рассмотрим только идеалы вида $H(p^k, h)$, где $\mathbb{Z}[x]/H(p^n, h)$ — конечное кольцо. Назовем многочлен h *хорошим*, если h не имеет вида $p^k s$ относительно некоторого простого числа p, $k \geqslant 1$.

Рассмотрим идеал $H(p^k, h)$, где h — хороший многочлен, p — простое число, $k \geqslant 1$, и разложим h в произведение попарно копростых неприводимых многочленов (лемма Гензеля, см. [3]):

$$h = f_1^{s_1} f_2^{s_2} \cdots f_k^{s_k}, \tag{4.1}$$

где f_i — неприводимые многочлены, $i = 1, 2, \ldots, k$. Хорошо известно, что кольцо $\mathbb{Z}[x]/H(p^n, h)$ изоморфно прямой сумме колец $\mathbb{Z}[x]/H(p^n, f_i^{s_i})$,

$$\mathbb{Z}[x]/H(p^n, h) \cong \bigoplus_{i=1}^{k} \mathbb{Z}[x]/H(p^n, f_i^{s_i}). \tag{4.2}$$

Обозначим эти кольца через $V_k(p^n, f^s) = \mathbb{Z}[x]/H(p^n, f^s)$, где $k = \deg f$, $1 \leqslant n$, $s \in \mathbb{N}$, а f — неприводимый многочлен $\bmod p$. Ясно, что $V_k(p^n, f^s)$ — также (неточный) $\mathbb{Z}[x]$-модуль. Поскольку f неприводим, то содержание f эквивалентно 1, а старший коэффициент $a_0(f)$ относительно прост с p, то можно считать, что $a_0(f) = 1$. Пусть M — точный локально конечный модуль над $A = \mathbb{Z}[x]$. Тогда для любого $m \in M$ имеем, что mA — конечный A-модуль и $\operatorname{An}(m) = \{a \in A \mid ma = 0\}$ — идеал в A. Пусть $q = \operatorname{char}(mA)$ — аддитивный показатель конечной абелевой группы mA. Тогда $mA \cong \mathbb{Z}[x]/\operatorname{An}(m)$, где идеал $\operatorname{An}(m)$ может быть рассмотрен как $\operatorname{An}(m) = H(q, f)$ для некоторого f. Поскольку кольцо $\mathbb{Z}[x]$ нетерово, то $\operatorname{An}(m)$ конечно порожден. Так как $\mathbb{Z}[x]$ — факториальное кольцо, то можно обозначить через l наименьшее общее кратное образующих. Тогда $H(q, l) \subset \operatorname{An}(m)$ и $\mathbb{Z}[x]/\operatorname{An}(m)$ есть гомоморфный образ A-модуля $\mathbb{Z}[x]/H(q, l)$. Пусть $q = p_1^{r_1} \cdots p_m^{r_m}$ — простое разложение q. В кольце $\mathbb{Z}[x]/H(p_i^{r_i}, l)$ выберем разложение l типа (4.1) $\bmod p_i$, т.е. $l = f_1^{s_1} \cdots f_t^{s_t}$, с попарно копростыми неприводимыми многочленами $\bmod p_i$. Тогда A-модуль $\mathbb{Z}[x]/H(q, l)$ допускает прямое разложение

$$\mathbb{Z}[x]/H(q, l) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{t} V_{k_j}(p^{r_i}, f_j^{s_j}), \tag{4.3}$$

где $V_{k_j}(p^{r_i}, f_j^{s_j}) = \mathbb{Z}[x]/H(p^{r_i}, f_j^{s_j})$ и $k_j = \deg f_j$. Эти рассуждения показывают, что достаточно рассмотреть A-модули типа $V_k(p^m, f^s)$, $1 \leqslant k, m, s \in \mathbb{N}$, p — простое число, f неприводим $\bmod p$, а $a_0(f) = 1$.

Лемма 4.1. *Любой элемент A-модуля $V_k(p^m, f^s)$ есть $a\mathbb{Z}/p^m Z$-линейная комбинация следующих элементов $\mathbb{Z}[x] \bmod p^m$ и $\bmod f^s$:*

$$\begin{array}{lll}
1, x, \ldots, x^{k-1}, & p, px, \ldots, px^{k-1}, & p^{m-1}, p^{m-1}x, \ldots, p^{m-1}x^{k-1} \\
f, xf, \ldots, x^{k-1}f, & pf, pxf, \ldots, px^{k-1}f, & p^{m-1}f, p^{m-1}xf, \ldots, p^{m-1}x^{m-1}f, \\
f^2, xf^2, \ldots, x^{k-1}f^2, & pf^2, pxf^2, \ldots, px^{k-1}f^2, & p^{m-1}f^2, p^{m-1}xf^2, \ldots, p^{m-1}x^{m-1}f^2, \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\
f^{s-2}, xf^{s-2}, \ldots, x^{k-1}f^{s-2}, & pf^{s-2}, pxf^{s-2}, \ldots, p^{k-1}f^{s-2}, & p^{m-1}f^{s-2}, p^{m-1}xf^{s-2}, \ldots, p^{m-1}x^{k-1}f^{s-2}, \\
f^{s-1}, xf^{s-1}, \ldots, x^{k-1}f^{s-1}, & pf^{s-1}, pxf^{s-1}, \ldots, px^{k-1}f^{s-1}, & p^{m-1}f^{s-1}, p^{m-1}xf^{s-1}, \ldots, p^{m-1}x^{k-1}f^{s-1}.
\end{array} \tag{4.4}$$

Доказательство. Любое число $0 < q < p^m$ имеет вид

$$q = \alpha_1 p^{m-1} + \alpha_2 p^{m-2} + \cdots + \alpha_{m-1} p + \alpha_m,$$

где $0 \leqslant \alpha_i < p - 1$, а любой полином h, где $\deg h \geqslant \deg f$, имеет вид

$$h = \varphi_1 f^{s-1} + \varphi_2 f^{s-2} + \cdots + \varphi_{s-1} f + \varphi_1,$$

где $\deg \varphi_i < \deg f$ и коэффициенты φ_i берутся $\bmod p^m$; поэтому

$$\varphi_i = \psi_{i_0} + p\psi_{i_1} + \ldots + p^{m-1}\psi_{i_{m-1}}.$$

Отсюда легко вытекает лемма. □

Лемма 4.2. *Существуют следующие соотношения между $\mathbb{Z}[x]$-модулями $V_k(p^m, f^s)$:*

1) *$V_k(p^m, f^{s-1})$ изоморфен $fV_k(p^m, f^s)$;*
2) *$V_k(p^{m-1}, f^s)$ изоморфен $pV_k(p^m, f^s)$;*

3) $V_k(p^{m-1}, f^{s-1})$ *изоморфен* $pfV_k(p^m, f^s)$;
4) $V_k(p^r, f^l)$, *где* $r < m$ *и* $l < s$, *изоморфен* $p^{m-r}f^{s-l}V_k(p^m, f^s)$.

Доказательство. (1) Согласно лемме 4.1, $V_k(p^m, f^{s-1})$ порожден элементами (4.4) без последней строки. После умножения на элемент f элементы (4.4) $(\mathrm{mod}\, p^s)$ становятся элементами (4.4) без первой строки. Тогда легко видеть, что любой элемент $fV_k(p^m, f^{s-1})$ имеет вид $f \cdot h$, где h — произвольный элемент $V_k(p^m, f^{s-1})$. Определим $\mathbb{Z}[x]$-линейное отображение

$$\pi_f : V_k(p^m, fs-1) \to V_k(p^m, f^s), \quad h \mapsto f \cdot h.$$

Пусть $g \in \mathbb{Z}[x]$. Тогда $h \cdot g(\mathrm{mod}\, f^{s-1})$ — элемент $V_k(p^m, f^{s-1})$ и $(fh \circ g)(\mathrm{mod}\, p^s)$ — элемент $V_k(p^m, f^s)$. Ясно, что

$$\pi_f(h \circ g)(\mathrm{mod}\, f^{s-1}) \equiv (fh \circ g)(\mathrm{mod}\, f^s).$$

Это означает, что

$$\pi_f(h \circ g) \equiv \pi_f(h \circ g)(\mathrm{mod}\, f^{s-1}) = fhg(\mathrm{mod}\, p^s) = f(hg)(\mathrm{mod}\, p^s) = (fh \circ g)(\mathrm{mod}\, p^s) = \pi_f(h) \circ g.$$

Это доказывает (1). (2) может быть доказано аналогично (1). (3) и (4) следуют из (1) и (2) последовательным применением проведенных рассуждений (итерация). □

Лемма 4.3. *Любой конечно порожденный подмодуль локально конечного* $\mathbb{Z}[x]$*-модуля* M *изоморфен конечной прямой сумме* $\mathbb{Z}[x]$*-модулей типа* $V_k(p^m, f^s) = \mathbb{Z}[x]/H(p^m, f^s)$ *или гомоморфному образу* $\mathbb{Z}[x]$*-модулей такого типа, где* p *— простое число,* $m \geqslant 0$, $s \geqslant 1$, *а* f *— неприводимый многочлен* $\mathrm{mod}\, p$.

Доказательство. Это следует из рассмотрений, предшествующих лемме 4.1. Для любых $a_1, \ldots, a_s \in M$ любой подмодуль $a_i\mathbb{Z}[x]$ изоморфен $\mathbb{Z}[x]$-модулю типа $V_{k_i}(m_i, h_i)$ или гомоморфному образу такого модуля. Тогда подмодуль $\sum a_i\mathbb{Z}[x]$ изоморфен прямой сумме $\bigoplus\limits_{i=1}^{s} V_{k_i}(m_i, h_i)$ или гомоморфному образу $\mathbb{Z}[x]$-модулей такого типа. Тогда используем разложение (4.3). □

Теорема 4.4. *Подкатегория локально конечных модулей в* $\mathbb{Z}[x]$-Mod *порождена* $\mathbb{Z}[x]$*-модулями*

$$\big\{V_k(p^m, f^s) \mid p \text{ — простое число, } f \text{ неприводим, } 1 \leqslant k = \deg f,\ m, s \in \mathbb{N}\big\}.$$

Доказательство следует из леммы 4.3.

Отметим одно специальное свойство $\mathbb{Z}[x]$-модулей $V_k(p^m, f^s)$. Элементы этого модуля имеют аддитивный порядок p^l, где $l \leqslant m$, и «мультипликативный» порядок f^i, где $i \leqslant s$. Это означает, что $f^s p^m V_k(p^m, f^s) = 0$. Поэтому $V_k(p^m, f^s)$ называется $\mathbb{Z}[x]$*-модулем с* (p, f)*-кручением*. Согласно лемме 4.2, рассмотрим локально конечный $\mathbb{Z}[x]$-модуль

$$V(p^\infty, f^\infty) = \bigcup_{i=1}^{\infty} V_k(p^i, f^i).$$

Лемма 4.5. *Локально конечный* $\mathbb{Z}[x]$*-модуль* $V(p^\infty, f^\infty)$ *имеет бесконечно много неприводимых* $\mathbb{Z}[x]$*-подмодулей. Все неприводимые подмодули содержат простой* $\mathbb{Z}[x]$*-подмодуль* $V_k(p, f)$. *Модуль* $V(p^\infty, f^\infty)$ *неприводим.*

Доказательство. Лемма 4.1 позволяет записать

$$V(p^\infty, f^m) = \bigcup_{i=s\geqslant 1}^{\infty} V_k(p^i, f^m), \quad V_k(p^s, f^\infty) = \bigcup_{j=d\geqslant 1}^{\infty} V_k(p^s, f^j),$$

где $s \geqslant 1$, $m \geqslant 1, k = \deg f$, f неприводим, p — простое число и

$$V_k(p^\infty, f^\infty) = \bigcup_{\substack{i+j\geqslant t \\ t\geqslant 2}}^{\infty} \left\{ V_k(p^{i,j}) \;\middle|\; \begin{array}{l} \text{после } (i,j) \text{ следующий шаг — к } (i+1,j) \text{ или} \\ (i, j+1) \text{ (берется только одна из этих пар)} \end{array} \right\}.$$

Например, после $V_k(p^i, f^j)$ для следующего шага берется $V_k(p^{i+1}, f^j)$ или $V_k(p^i, f^{j+1})$, поскольку $V_k(p^i, f^j) \subset V_k(p^{i+1}, f^j)$ и $V_k(p^i, f^j) \subset V_k(p^i, f^{j+1})$ неприводимы и содержатся в $V_k(p^\infty, f^\infty)$. По построению $\mathbb{Z}[x]$-модуля $V_k(p^\infty, f^\infty)$ этот модуль локально конечен и точен. □

Пусть $A = \mathbb{Z}[x]$. Поле рациональных дробей $\mathbb{Q}(x) = Q(\mathbb{Z}[x])$ инъективно в категории правых A-модулей, что проверяется непосредственно.

Рассмотрим теперь A-модуль $\overline{\mathbb{Q}(x)} = \mathbb{Q}(x)/\mathbb{Z}[x]$. Заметим, что этот A-модуль состоит из конечных сумм рациональных функций типа

$$\frac{m}{p^k},\ \frac{h}{p^k},\ \frac{\varphi}{p^k f^r},\ \frac{n}{f^l},\ \frac{\psi}{f^l},$$

где p — простое число, f — неприводимый и примитивный многочлен, $1 \leqslant m < p$, $\deg\varphi < \deg f$, $\deg\psi < \deg f$, коэффициенты h и φ меньше, чем p, а $n \in \mathbb{N}$. Из дробей типов n/f^l и ψ/f^l построим A-подмодуль H и рассмотрим фактормодуль $\overline{\overline{\mathbb{Q}(x)}} = \overline{\mathbb{Q}(x)}/H$.

Лемма 4.6. *A-модули $\overline{\mathbb{Q}(x)}$ и $\overline{\overline{\mathbb{Q}(x)}}$ инъективны в категории A-модулей.*

Доказательство. (i) Пусть I — идеал кольца $A = \mathbb{Z}[x]$. Ясно, что он имеет вид

$$I = mA + f_1A + \cdots + f_kA,$$

где $0 \leqslant m \in \mathbb{Z}$ и f_i — многочлены из $\mathbb{Z}[x]$. Пусть $\iota : I \to \mathbb{Z}[x]$ — инъекция и $\varphi : I \to \overline{\mathbb{Q}(x)}$ — произвольный гомоморфизм A-модулей. Нужно доказать существование гомоморфизма $\pi : \mathbb{Z}[x] \to \overline{\mathbb{Q}(x)}$ такого, что $\pi \circ \iota = \varphi$. Это эквивалентно равенствам

$$\begin{cases} \varphi(m) = \pi(1) \cdot m, \\ \varphi(f_i) = \pi(1) f_i, \qquad \text{где } 1 \in \mathbb{Z},\ i = 1, 2, \ldots, k. \end{cases} \tag{4.5}$$

Далее, φ удовлетворяет условиям

$$\pi(mf_1 \cdots f_k) = \varphi(m) f_1 \cdots f_k = \varphi(f_1) m \cdots f_k = \cdots = \varphi(f_k) m f_1 \cdots f_{k-1}. \tag{4.6}$$

Пусть $\varphi(mf_1 \cdots f_k) = d/q$, где $d, q \in \mathbb{Z}[x]$. Тогда в силу (4.5) и (4.6) имеем

$$\pi(1) m f_1 f_2 \cdots f_k = \frac{d}{q}, \tag{4.7}$$

где d/q зависит от гомоморфизма φ. В силу (4.6) и (4.7) можно определить

$$\pi(1) = \frac{d}{q \cdot m f_1 f_2 \cdots f_k}.$$

Ясно, что $\pi(1)$ удовлетворяет (4.5).

(ii) Пусть $I = mA + f_1A + \cdots + f_kA$ — произвольный идеал в $A = \mathbb{Z}[x]$ с инъекцией $\iota : I \to \mathbb{Z}[x]$. Нужно показать, что для любого гомоморфизма $\varphi : I \to \overline{\overline{Q(x)}}$ существует гомоморфизм $\pi : \mathbb{Z}[x] \to \overline{\overline{\mathbb{Q}(x)}}$ такой. что $\varphi = \pi \circ \iota$. Это условие эквивалентно следующим равенствам в $\overline{\overline{\mathbb{Q}(x)}}$:

$$\varphi(m) = \frac{\varphi_0}{m_0\psi_0} = \pi(1) m, \quad \varphi(f_i) = \frac{\varphi_i}{m_i\psi_i} = \pi(1) f_i, \tag{4.8}$$

где $i = 1, 2, \ldots, k$. Далее, φ удовлетворяет условиям

$$\varphi(mf_1 \cdots f_k) = \varphi(m) f_1 \cdots f_k = \varphi(f_1) m \cdots f_k = \cdots = \varphi(f_k) m f_1 \cdots f_{k-1}. \tag{4.9}$$

Пусть

$$\varphi(mf_1 \cdots f_k) = \frac{h}{s}, \tag{4.10}$$

где $h/s \in \overline{\overline{\mathbb{Q}(x)}}$, и зависит от гомоморфизма φ. В силу (4.8)–(4.10), имеем равенство

$$\pi(1) m f_1 f_2 \cdots f_k = \frac{h}{s}$$

и, следовательно, можно определить

$$\pi(1) = \frac{h}{smf_1f_2\cdots f_k}. \tag{4.11}$$

В силу (4.8), имеем

$$\frac{\varphi_0}{mm_0\psi_0} = \frac{h}{smf_1f_2\cdots f_k} = \frac{\varphi_i}{m_i\psi_i f_i}, \tag{4.12}$$

и получается, что аддитивные порядки элементов $\varphi(m)$ и $\varphi(f_i)$ равны соответственно m_0 и m_i. Пусть l — наименьшее общее кратное $m_0, m_1, \ldots, m_k$. Если умножить (11) на $m \cdot l$, то $\dfrac{l\cdot h}{sf_1f_2\cdots f_k} = 0$ в $\overline{\overline{\mathbb{Q}(x)}}$ и $\dfrac{lh}{s} = \dfrac{d}{rq}$, где q примитивно. Поэтому имеем $\dfrac{h}{s} = \dfrac{d}{rlq}$, где $l = [m_0, m_1, \ldots, m_k]$, q примитивно и $\pi(1) = \dfrac{d}{rlqmf_1\cdots f_k}$. Это доказывает лемму. □

Введем обозначение $F(x) = \overline{\overline{\mathbb{Q}(x)}}$. Ясно, что любой элемент A-модуля $F(x)$ есть конечная сумма элементов вида

$$z_{p,f} = \sum_{i=1}^{s}\frac{m_i}{p^{k_i}} + \sum_{i=1}^{n}\frac{h_i}{p^{l_i}} + \sum_{i=1}^{d}\frac{\varphi_i}{p^{n_i}f^{s_i}}, \tag{4.13}$$

где p — простое число, многочлен f неприводим и примитивен, $0 \leqslant m_i < p$, $\deg\varphi_i < \deg f$, а коэффициенты h_i и φ_i меньше, чем p. Заметим, что $F(x)$ — локально конечный A-модуль, а а $F(x)$ — абелева группа с кручением.

Рассмотрим следующие два подмножества $M(x)$ и $L(x)$ A-модуля $F(x)$:

$$M(x) = \Big\{ \sum_{p,f} z_{p,f} \in F(x) \;\Big|\; z_{p,f} \text{ имеет тип (4.13), } a_0(f) = 1,\ f \text{ неприводим} \Big\},$$

$$L(x) = \left\{ \sum_{i,j}\frac{\phi_{ij}}{p_i^{n_i}f_j^{s_j}} \in F(x) \;\middle|\; \begin{array}{l} p_i \text{ — простые числа, } a_0(f_j) \neq 1,\ f_j \text{ — неприводимые} \\ \text{многочлены такие, что } \deg\phi_{ij} < \deg f_j, \text{ а коэффи-} \\ \text{циенты } \phi_{ij} \text{ меньше, чем } p_i\text{ю} \end{array} \right\}.$$

Лемма 4.7. *$M(x)$ и $L(x)$ — подмодули $F(x)$ и $F(x) = M(x) \oplus L(x)$.*

Доказательство. Ясно, что $M(x)$ и $L(x)$ замкнуты относительно сложения; докажем, что они замкнуты относительно умножения на элементы кольца $A = \mathbb{Z}[x]$.

Пусть $r = \sum \dfrac{\phi_{ij}}{p_n^i f_j^{s_j}} \in L(x)$ и $h \in A$. Покажем, что $h \cdot r \in L(x)$. Это достаточно доказать для одного слагаемого вида $\dfrac{\phi}{p^n f^s}$ в r. В случае, когда $\deg h\phi < \deg f$, видим, что $\dfrac{h\phi}{p^n f^s}$ содержится в $L(x)$. Пусть теперь $\deg h\phi \geqslant \deg f$, $a_0(f) = b$, $\deg h\phi = m$, а $\deg f = k$. Рассмотрим элемент

$$\frac{h\phi}{p^n f^s} = \frac{b_0^{m-k}h\phi}{p^n b_0^{m-k} f^s} \tag{4.14}$$

и следующее разложение $p^n b_0^{m-k}$ на простые сомножители:

$$p^n b_0^{m-k} = p^{k_1}p_2^{k_2}\ldots p_d^{k_d},$$

где $p = p_1$, p_2, …, p_d — простые числа. С помощью стандартных рассуждений можно представить элемент (4.14) в виде

$$\frac{h\phi}{p^n f^s} = \sum_{i=1}^{d}\frac{v_i b_0^{m-n}h\phi}{p_i^{k_i}f^s}. \tag{4.15}$$

В силу алгоритма Евклида многочлен $b_0^{m-n}h\phi$ может быть представлен в виде суммы степеней f:

$$b_0^{m-k}h\phi = \phi_0 f^r + \phi_1 f^{r-1} + \phi_{r-1}f + \phi_r, \tag{4.16}$$

где $\deg\phi_r < \deg f$.

Подставляя (4.16) в (4.15), имеем

$$\frac{h\phi}{p^n f^s} = \sum_{j=0}^{r} \sum_{i=1}^{d} \frac{v_i \phi_j}{p_i^{k_i} f^{s_j}}. \tag{4.17}$$

Это доказывает, что $L(x)$ есть A-модуль.

Далее покажем, что $M(x)$ есть A-модуль. С этой целью достаточно доказать, что для любых $h \in A$ и $z_{p,f} \in M(x)$ произведение $z_{pf} \cdot h$ содержится в $M(x)$.

Рассмотрим следующие три случая:

$$\text{(a)} \quad z_{p,f} = \sum_{i=0}^{s} \frac{m_i}{p^{k_i}}; \qquad \text{(b)} \quad zp, f = \sum_{i=1}^{n} \frac{h_i}{p^{l_i}}; \qquad \text{(c)} \quad z_{p,f} = \sum_{i=1}^{d} \frac{\phi_i}{p^{n_i} f^{s_i}}.$$

В случаях (a) и (b) имеем

$$z_{p,f} \cdot h = \sum_{i=1}^{n} \frac{m_i \cdot h}{p^{k_i}}, \quad z_{,f} \cdot h = \sum_{i=1}^{n} \frac{h_i h}{p^{l_i}},$$

где оба элемента, очевидно, содержатся в $M(x)$. В случае (c)

$$z_{p,f} \cdot h = \sum_{i=1}^{d} \frac{\varphi_i h}{p^{n_i} f^{s_i}} \sum_{i=1}^{d} \sum_{j=0}^{q} \frac{\psi_{ij}}{p^{n_i} f^{s_i}}, \tag{4.18}$$

где

$$\varphi_i h = \psi_{i0} + \psi_{i1} f + \psi_{i2} f^2 + \ldots + \psi_{iq_i} f^{q_i},$$

$i = 1, 2, \ldots, d$, $\deg \psi_{ij} < \deg f$, а коэффициенты ψ_{ij} меньше, чем p.

Равенство (4.18) означает, что $z_{p,f} h \in M(x)$ и, следовательно, $M(x)$ есть A-модуль и $F(x) = M(x) \oplus L(x)$.

Заметим, что $M(x)$ и $L(x)$ — инъективные A-модули как прямые слагаемые инъективного модуля $\overline{\overline{Q(x)}}$ (см. лемму 4.6). □

Пусть $M_p(x)$ — p-компонента A-модуля $M(x)$,

$$M_p(x) = \{z \in M(x) \mid p^k z = 0 \text{ для некоторого } k \in \mathbb{N}\},$$

где p — простое число. Ясно, что

$$M(x) = \bigoplus_p M_p(x)$$

и элемент z в $M_p(x)$ имеет вид $z = z_{p,f_1} + z_{p,f_2} + \cdots + z_{p,f_k}$.

Лемма 4.8. *Для любого простого числа p локально конечный $\mathbb{Z}[x]$-модуль*

$$H_p(f) = \sum_{k=1}^{\infty} \sum_{f} V_k(p^\infty, f^\infty),$$

где f — неприводимые примитивные многочлены с $a_0(f) = 1$, изоморфен $\mathbb{Z}[x]$-модулю $M_p(x)$.

Доказательство. Согласно лемме 4.2(3) любой элемент $h \in H_p(f)$ имеет вид

$$h = \sum_{i=1}^{m} p^{n_i} \mu_i f_1^{k_i} + \sum_{i=1}^{n} p^{m_i} \nu_i f_2^{s_i} + \cdots + \sum_{i=1}^{k} p^{l_i} \chi_i f_q^{r_i}, \tag{4.19}$$

где $n_i, m_i, \ldots, l_i \in \mathbb{N}$, $k_i, s_i, \ldots, r_i \in \mathbb{N}_0$, $\deg \mu_i < \deg f_1$, $\deg \nu_i < \deg f_2$, …, $\deg \chi i < \deg f_q$, коэффициенты многочленов ν_i, μ_i, χ_i меньше, чем p, f_i — неприводимые примитивные многочлены,

а $a_0(f_i) = 1, i = 1, 2, \ldots, q$. Пусть

$$m_0 = \max\{n_i, m_j, \ldots, l_r \mid i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n,\ \ldots,\ r = 1, 2, \ldots, k\},$$
$$l_0 = \min\{n_i, m_j, \ldots, l_r \mid i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n,\ \ldots,\ r = 1, 2, \ldots, k\},$$
$$n_0^{(1)} = \max\{k_i \mid i = 1, 2, \ldots, m\}, \quad n_0^{(2)} = \max\{s_j \mid i = 1, 2, \ldots, n\}, \quad \ldots,$$
$$n_0^{(q)} = \max\{r_i \mid i = 1, 2, \ldots, k\}, \quad n_0 = \max\{n_0^{(1)}, n_0^{(2)}, \ldots, n_0^{(q)}\}.$$

Тогда элемент h содержится в $\sum\limits_{i=1}^{q} V_{t_i}(p^{m_0+1}, f_i^{n_0^{(i)}+1})$, где $t_i = \deg f_i$ и аддитивный порядок h равен $p^{m_0-l_0+1}$.

Определим линейное отображение $\Phi : H_p(f) \to M_p(x)$ формулой

$$\Phi(h) = \sum_{i=1}^{m} \frac{\mu_i}{p^{m_0-n_i} f_1^{n_0^{(1)}-k_i}} + \sum_{i=1} n \frac{\nu_i}{p^{m_0-m_i} f_2^{n_0^{(2)}-s_i}} + \cdots + \sum \frac{\chi i}{p^{m_0-l_i} f_q^{n_0^{(q)}-r_i}}. \tag{4.20}$$

Ясно, что Φ — инъективное отображение. Покажем, что Φ есть гомоморфизм A-модулей. В силу линейности Φ достаточно рассмотреть только одно слагаемое в (4.19), например, $h_1 = \sum\limits_{i=1}^{m} p^{n_i} \mu_i f_1^{k_i}$, где $h_1 \in V_{t_1}(p^{m_0+1}, f_1^{n_0^{(1)}+1})$. Кроме того, достаточно рассмотреть действие полиномов из $A = \mathbb{Z}[x]$ типа $\phi = \psi f_1^d$ или $\phi = p^{d_1} \psi f_1^{d_2}$, где $d, d_i \geqslant 0$, $\deg \psi < \deg f_1$, а коэффициенты ψ меньше, чем p. В $H_p(f)$ имеем

$$h_1 \psi f_1^d = \sum_{i=1}^{m} p^{n_i} \mu_i \psi f_1^{k_i+d} = \sum_{i=1}^{m} \sum_{s=0}^{k} p^{n_i} h_i^{(s)} f_1^{k_i+d+s}, \tag{4.21}$$

где

$$\mu_i \psi = \sum_{s=0}^{k} h_i^{(s)} f_1^s. \tag{4.22}$$

Тогда образ элемента (4.21) есть

$$\Phi(h_1 \psi f_1^d) = \Phi\left(\sum_{i=1}^{m} \sum_{s=0}^{k} p^{n_i} h_i^{(s)} f_1^{k_i+d+s} \right) = \sum_{i=1}^{m} \sum_{s=0}^{k} \frac{h_i^{(s)}}{p^{m_0-n_i} f_1^{n_0^{(1)}-k_i-d-s}}. \tag{4.23}$$

Используя равенство в $M_p(x)$, имеем

$$\begin{aligned} \Phi(h_1)(\psi f_1^d) &= \sum_{i=1}^{m} \frac{\mu_i \psi f_1^d}{p^{m_0-n_i} f_1^{n_0^{(i)}-k_i}} = \sum_{i=1}^{m} \frac{\sum\limits_{s=1}^{k} h_i^{(s)} f_i^{s+d}}{p^{m_0-n_i} f_1^{n_0^{(1)}-x_i}} = \\ &= \sum_{i=1}^{m} \sum_{s=0}^{k} \frac{h_i^{(s)}}{p^{m_0-n_i} f_1^{n_0^{(1)}-k_i-d-s}}. \end{aligned} \tag{4.24}$$

Из уравнений (4.23) и (4.24), заключаем, что

$$\Phi(h_1 \cdot (\psi f_1^d)) = \Phi(h_1) \cdot (\psi f_1^d). \tag{4.25}$$

Рассмотрим теперь действие многочленов типа $p^r \psi \cdot f_1^d$ на h_1 и $\Phi(h_1)$, как и выше. Тогда, используя уравнение (4.22) в $H_p(f)$, получаем

$$\begin{aligned} h_1(p^r \psi f_1^d) &= \sum_{i=1}^{m} p^{n_i+r} \mu_i \psi f_1^{k_i+d} = \sum_{i=1}^{m} \sum_{s=0}^{k} p^{n_i+r} h_i^{(s)} f_1^s f_1^{k_i+d} = \\ &= \sum_{i=1}^{m} \sum_{s=0}^{k} p^{n_i+r} h_i^{(s)} f_1^{k_i+d+s}. \end{aligned} \tag{4.26}$$

Образ (4.26) при отображении Φ есть

$$\Phi(h_1(p^r\psi f_1^d)) = \sum_{i=1}^{m}\sum_{s=0}^{k} \frac{h_i^{(s)}}{p^{m_0-n_i-r} f_1^{n_0^{(1)}-k_i-d-s}}. \tag{4.27}$$

Рассмотрим в $M_p(x)$ действие $p^r\psi f_1^d$ на элемент $\Phi(h_1)$. В силу (4.22) имеем

$$\begin{aligned}\Phi(h_1)\cdot(p^r\psi f_1^d) &= \sum \frac{\mu_i p^r \psi f_1^d}{p^{m_0-n_i} f_1^{n_0^{(1)}-k_i}} = \sum \frac{\mu_i \psi}{p^{m_0-n_i-r} f_1^{n_0^{(1)}-k_i-d}} = \\ &= \sum_{i=0}^{m}\sum_{s=0}^{k} \frac{h_i^{(s)} f_1^s}{p^{m_0-n_i-r} f_1^{n_0^{(1)}-k_i-d}} = \sum_{i=1}^{m}\sum_{s=0}^{k} \frac{h_i^{(s)}}{p^{m_0-n_i-r} f_1^{n_0^{(1)}-k_i-d-s}}\end{aligned} \tag{4.28}$$

Равенства (4.27) и (4.28) дают

$$\Phi(h_1(p^r\psi f_1^d)) = \Phi(h_1)(p^r\psi f_1^d). \tag{4.29}$$

В силу (4.25) и (4.29) заключаем, что Φ — морфизм A-модулей. Это доказывает лемму. □

Теорема 4.9. *Справедливы следующие утверждения в подкатегории локально конечных модулей в* $\mathbb{Z}[x]$-Mod:

1) $\mathbb{Z}[x]$*-модуль* $M(x)$ *инъективен и*

$$M(x) \cong \bigoplus_p \sum_f \sum_{k=1}^{\infty} V_k(p^\infty, f^\infty),$$

где p *— простые числа, а* f *— неприводимые примитивные многочлены и* $a_0(f) = 1$;

2) $\mathbb{Z}[x]$*-модули*

$$H_p(f) = \sum_f \sum_{k=1}^{\infty} V_k(p^\infty, f^\infty) \cong M_p(x)$$

инъективны;

3) $\mathbb{Z}[x]$*-модуль* $M(x)$ *есть когенератор в подкатегории всех локально конечных модулей, а сама эта подкатегория не является конечно порожденной.*

Доказательство. Ясно, что $M(x) = \bigoplus_p M_p(x)$. В лемме 4.8 был получен изоморфизм

$$M_p(x) \cong \sum_{(f)} \sum_{k=1}^{\infty} V_k(p^\infty, f^\infty).$$

Отюда вытекает справедливость 1).

Согласно леммам 4.6 и 4.7 $M(x)$ инъективен; прямые слагаемые $\sum_f \sum_{k=1}^{\infty} V_k(p^\infty, f^\infty)$ — инъективные $\mathbb{Z}[x]$-модули. Любой простой $V_k(p,f)$-модуль вкладывается в $M_p(x)$ и, следовательно, $M(x)$ является кообразующей. Очевидно, что рассматриваемая подкатегория не является конечно порожденной. □

СПИСОК ЛИТЕРАТУРЫ

1. *Львов И. В.* О многообразиях ассоциативных колец. I// Алгебра и логика. — 1973. — *12*, № 3. — С. 269–297.
2. *Lewin J.* Subrings of finite index of finitely generated rings// J. Algebra. — 1967. — *5*. — С. 84–88.
3. *McDonald B. R.* Finite rings with identity. — N.Y.: Marcel Dekker, 1974.
4. *Mekei A.* On the varieties of finitely approximable rings// Sci. J. Nat. Univ. Mongol. — 2000. — *7*. — С. 3–13.

5. *Orzech M., Riber L.* Residual finiteness and Hopfian property in rings// J. Algebra. — 1970. — *15*. — C. 81–88.
6. *Wisbauer R.* Foundations of module and ring theory. — Philadelphia: Gordon and Breach, 1991.

А. Мекей
Department of Mathematics, National University of Mongolia, Ulaanbataar
E-mail: mekei@yahoo.com, mekeia@mail.ru

Р. Висбауэр
Department of Mathematics, Heinrich-Heine-University, Düsseldorf, Germany
E-mail: wisbauer@math.uni-duesseldorf.de

Современная математика и ее приложения. Том 14 (2004). С. 86–99

УДК 512.54

НЕКОММУТАТИВНЫЕ ГРУППЫ ПОРЯДКА 16 И ИХ ПОЛУГРУППЫ ЭНДОМОРФИЗМОВ

© 2004 г. **П. ПУУСЕМП**

Аннотация. Доказывается, что каждая конечная группа порядка 16 определяется своей полугруппой эндоморфизмов в классе всех групп.

СОДЕРЖАНИЕ

1. Введение

Хорошо известно, что множество всех эндоморфизмов абелевой группы образует кольцо, и многие свойства этой группы характеризуются свойствами ее кольца эндоморфизмов. Множество эндоморфизмов произвольной группы образует только полугруппу. Теория полугрупп эндоморфизмов групп мало развита. Во многих своих работах мы старались описать некоторые свойства заданной группы по свойствам ее полугруппы эндоморфизмов. Например, в [1,10] доказано, что прямое произведение групп и некоторые полупрямые произведения групп описываются свойствами их полугрупп эндоморфизмов. В [6] доказано, что во многих случаях суммируемость двух эндоморфизмов группы характеризуется свойствами полугруппы эндоморфизмов этой группы. Доказано также, что группы из многих известных классов групп определяются их полугруппами эндоморфизмов в классе всех групп. Примерами таких групп служат конечные абелевы группы [1, теорема 4.2], непериодические делимые абелевы группы [7, теорема 1], обобщенные группы кватернионов [2, следствие 1]. С другой стороны, известно много примеров групп, которые не определяются их полугруппами эндоморфизмов. Например, общеизвестен следующий результат А. Л. Корнера [4]: каждое счетное редуцированное кольцо с единицей и без кручения является кольцом эндоморфизмов континуального числа счетных редуцированных абелевых групп без кручения. Существуют и другие примеры такого типа: знакопеременная группа A_4 порядка 12 [8, теорема 4.1], некоторые полупрямые произведения конечных циклических групп [9, теорема 1]. Следовательно, полезно знать и другие примеры групп, которые определяются или не определяются их полугруппами эндоморфизмов. В настоящей работе мы рассмотрим группы порядка 16 и докажем следующую теорему.

Теорема. *Каждая группа порядка* 16 *определяется своей полугруппой эндоморфизмов в классе всех групп.*

Работа выполнена при поддержке Эстонского научного Фонда (проект № 4291 (2000-2003)).

ISSN 1512–1712

Будем придерживаться следующих обозначений:

G группа;
G' коммутант группы G;
$\mathrm{End}(G)$ полугруппа эндоморфизмов группы G;
$G = H \leftthreetimes K$ группа G является полупрямым произведением ее нормального делителя H и подгруппы K;
$\langle a, b, \ldots \rangle$ подгруппа группы G, порожденная ее элементами $a, b, \ldots$;
$\widehat{g}$ внутренний автоморфизм g;
$[a, b]$ коммутатор $[a, b] = a^{-1}b^{-1}ab$, $(a, b \in G)$;
$Z(G)$ центр группы G;
C_n циклическая группа порядка n;
D_n диэдральная группа порядка $2n$ $(n \geqslant 2)$:

$$D_n = \left\langle a, b \mid b^2 = a^n = 1,\ b^{-1}ab = a^{-1} \right\rangle;$$

Q_n обобщенная группа кватернионов порядка 2^{n+1} $(n \geqslant 2)$:

$$Q_n = \left\langle a, b \mid a^{2^n} = 1,\ b^2 = a^{2^{n-1}},\ b^{-1}ab = a^{-1} \right\rangle;$$

$Q = Q_2$ группа кватернионов;
$I(G)$ множество всех идемпотентов полугруппы $\mathrm{End}(G)$;
$[x]$ $= \{y \in I(G) \mid xy = y,\ yx = x\}$, $x \in I(G)$;
$K(x)$ $= \{y \in \mathrm{End}(G) \mid yx = xy = y\}$;
$V(x)$ $= \{y \in \mathrm{Aut}(G) \mid yx = x\}$;
$J(x)$ $= \{y \in \mathrm{End}(G) \mid yx = xy = 0\}$;
$H(x)$ $= \{y \in \mathrm{End}(G) \mid xy = y,\ yx = 0\}$.

Мы будем писать отображение справа от элемента, на которое оно действует. Если для заданной группы G из изоморфизма полугрупп $\mathrm{End}(G)$ и $\mathrm{End}(H)$, где H — некоторая другая группа, всегда следует изоморфизм групп G и H, то говорят, что группа G определяется своей полугруппой эндоморфизмов в классе всех групп.

2. Вспомогательные результаты

В этом разделе перечислим некоторые результаты, которые будут применяться в дальнейшем.

Лемма 2.1 (см. [1, теорема 4.2]). *Каждая конечная абелева группа определяется своей полугруппой эндоморфизмов в классе всех групп.*

Следовательно, для доказательства теоремы надо проверить утверждение теоремы только для некоммутативных групп порядка 16.

Лемма 2.2 (см. [1, теорема 1.13]). *Если группы A и B определяются своими полугруппами эндоморфизмов в классе всех групп, то и их прямое произведение $A \times B$ определяется своей полугруппой эндоморфизмов в классе всех групп.*

Лемма 2.3 (см. [2, следствие 1]). *Обобщенная группа кватернионов Q_n определяется своей полугруппой эндоморфизмов в классе всех групп.*

Лемма 2.4 (см. [8, следствие 3.7]). *Диэдральная группа D_{2^n} определяется своей полугруппой эндоморфизмов в классе всех групп для каждого $n \geqslant 1$.*

Лемма 2.5 (см. [11, теорема]). *Предположим, что группа G разлагается в полупрямое произведение $G = C_{p^n} \leftthreetimes C_m$, где p — простое число, n, m — некоторые положительные целые числа. Тогда группа G определяется своей полугруппой эндоморфизмов в классе всех групп.*

Перечислим теперь некоторые простые свойства полугруппы $\mathrm{End}(G)$, которые будут нужны в разделах 4 и 5 настоящей работы. Доказательство их элементарно.

Лемма 2.6. *Если $x \in I(G)$, то $G = \operatorname{Ker} x \leftthreetimes \operatorname{Im} x$ и $\operatorname{Im} x = \{g \in G \mid gx = g\}$.*

Лемма 2.7. *Если $y \in \operatorname{End}(G)$ и подгруппа $\operatorname{Im} y$ группы G абелева, то $\widehat{g} \in V(y)$ для каждого $g \in G$.*

Лемма 2.8. *Если $x, y \in \operatorname{End}(G)$ и $xy = yx$, то $(\operatorname{Im} x)y \subset \operatorname{Im} x$ и $(\operatorname{Ker} x)y \subset \operatorname{Ker} x$.*

Лемма 2.9. *Пусть $x \in I(G)$. Тогда*

$$K(x) = \{y \in \operatorname{End}(G) \mid (\operatorname{Im} x)y \subset \operatorname{Im} x,\ (\operatorname{Ker} x)y = \langle 1\rangle\}$$

и $K(x)$ является подполугруппой с единицей x в $\operatorname{End}(G)$, канонически изоморфной полугруппе $\operatorname{End}(\operatorname{Im} x)$. В этом изоморфизме элементу $y \in K(x)$ соответствует его ограничение на подгруппу $\operatorname{Im} x$.

Лемма 2.10. *Если $x \in I(G)$, то $[x] = \{y \in I(G) \mid \operatorname{Ker} x = \operatorname{Ker} y\}$.*

3. Некоммутативные группы порядка 16

Все некоммутативные группы порядка <32 описаны в [5, Table 1]. Некоммутативными группами порядка 16 являются следующие 9 групп (с точностью до изоморфизма):

- $\mathscr{G}_1 = C_2 \times D_4$;
- $\mathscr{G}_2 = C_2 \times Q$;
- $\mathscr{G}_3 = D_8$;
- $\mathscr{G}_4 = \langle a, b \mid b^2 = a^8 = 1,\ b^{-1}ab = a^3\rangle = \langle a\rangle \leftthreetimes \langle b\rangle \cong C_8 \leftthreetimes C_2$;
- $\mathscr{G}_5 = \langle a, b \mid b^2 = a^8 = 1,\ b^{-1}ab = a^5\rangle = \langle a\rangle \leftthreetimes \langle b\rangle \cong C_8 \leftthreetimes C_2$;
- $\mathscr{G}_6 = \langle a, b \mid b^4 = a^4 = 1,\ b^{-1}ab = a^{-1}\rangle = \langle a\rangle \leftthreetimes \langle b\rangle \cong C_4 \leftthreetimes C_4$;
- $\mathscr{G}_7 = \langle a, b \mid b^4 = a^4 = (ba)^2 = (b^{-1}a)^2 = 1\rangle$;
- $\mathscr{G}_8 = \langle a, b, c \mid a^2 = b^2 = c^2 = 1,\ abc = bca = cab\rangle$;
- $\mathscr{G}_9 = \langle a, b \mid a^4 = b^2 = (ab)^2\rangle$.

Лемма 3.1. *Группы $\mathscr{G}_7$, $\mathscr{G}_8$ и $\mathscr{G}_9$ можно описать следующим образом:*

$$\begin{aligned}
\mathscr{G}_7 &= \langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ bc = cb,\ ab = ba,\ c^{-1}ac = a^{-1}b\rangle \\
&= (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle \cong (C_4 \times C_2) \leftthreetimes C_2; \\
\mathscr{G}_8 &= \langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ ac = ca,\ b^{-1}cb = ca^2,\ b^{-1}ab = a^{-1}\rangle \\
&= (\langle a\rangle \times \langle c\rangle) \leftthreetimes \langle b\rangle \cong (C_4 \times C_2) \leftthreetimes C_2; \\
\mathscr{G}_9 &= \langle a, b \mid a^8 = 1,\ a^4 = b^2,\ b^{-1}ab = a^{-1}\rangle = Q_3.
\end{aligned}$$

Доказательство. Из определяющих соотношений группы $\mathscr{G}_7$ вытекает:

$$baba = 1, \quad b^{-1}ab^{-1}a = 1, \quad bab = b^{-1}ab^{-1}, \tag{3.1}$$

$$b^2a = ab^{-2} = ab^2, \quad b^2 \cdot b^{-1}ab = a^{-1}, \quad b^{-1}ab = a^{-1}b^2, \tag{3.2}$$

$$(ba)^{-1}a(ba) = a^{-1} \cdot b^{-1}ab \cdot a = a^{-1} \cdot a^{-1}b^2 \cdot a = a^{-1}b^2, \tag{3.3}$$

$$(ba)^{-1}b^2(ba) = a^{-1} \cdot b^{-1}b^2b \cdot a = b^2. \tag{3.4}$$

Следовательно,

$$\mathscr{G}_7 = (\langle a\rangle \times \langle b^2\rangle) \leftthreetimes \langle ba\rangle\,. \tag{3.5}$$

Обозначим элементы b^2 и ba через b и c соответственно. Тогда из формул (3.1)–(3.5) следует первое утверждение леммы.

Рассмотрим теперь определяющие соотношения группы $\mathscr{G}_8$. Из них вытекает:

$$ab \cdot c = c \cdot ab, \quad babc = ca, \quad bab = cac, \quad ab \cdot ab = a \cdot cac = acac, \tag{3.6}$$

$$ab \cdot ab \cdot ab = acacab = acaabc = acbc = acbcaa = accaba = ba. \tag{3.7}$$

Поэтому

$$(ab)^4 = ab \cdot ba = 1, \quad \langle c, ab\rangle = \langle c\rangle \times \langle ab\rangle, \quad \mathscr{G}_8 = \langle c, a, b\rangle = \langle c, a, ab\rangle.$$

По формулам (3.6) и (3.7)

$$a^{-1} \cdot c \cdot a = aca = acacc = (ab)^2 \cdot c, \tag{3.8}$$

$$a^{-1} \cdot ab \cdot a = ba = (ab)^3 = (ab)^{-1}. \tag{3.9}$$

Следовательно,

$$\mathscr{G}_8 = (\langle ab\rangle \times \langle c\rangle) \leftthreetimes \langle a\rangle \cong (C_4 \times C_2) \leftthreetimes C_2. \tag{3.10}$$

Обозначим элементы ab и a через a и b соответственно. Тогда из формул (3.8)–(3.10) следует второе утверждение леммы.

Наконец, рассмотрим определяющие соотношения группы $\mathscr{G}_9$. Из них вытекает:

$$b^2 = abab, \quad aba = b, \quad b^{-1}ab = a^{-1},$$

$$b^{-1}a^4b = a^{-4}, \quad b^{-1}b^2b = a^{-4}, \quad b^2 = a^{-4}, \quad a^4 = a^{-4}, \quad a^8 = 1.$$

Поэтому

$$\mathscr{G}_9 = \left\langle a, b \mid a^8 = 1,\ a^4 = b^2,\ b^{-1}ab = a^{-1}\right\rangle = Q_3.$$

Лемма доказана. □

Из утверждений лемм 2.1–2.5 ясно, что группы $\mathscr{G}_1$–$\mathscr{G}_6$ и $\mathscr{G}_9$ определяются своими полугруппами эндоморфизмов в классе всех групп. В следующих двух частях настоящей статьи доказывается, что группы $\mathscr{G}_7$ и $\mathscr{G}_8$ также определяются своими полугруппами эндоморфизмов в классе всех групп.

4. Описание группы $\mathscr{G}_7$ ее полугруппой эндоморфизмов

Обозначим всюду в этом разделе $G = \mathscr{G}_7$. Согласно лемме 3.1

$$G = \langle a, b, c\rangle = (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle \cong (C_4 \times C_2) \leftthreetimes C_2,$$

где

$$a^4 = b^2 = c^2 = 1, \quad bc = cb, \quad ab = ba, \quad c^{-1}ac = a^{-1}b. \tag{4.1}$$

Из (4.1) вытекает

$$c^{-1}a^2c = a^{-2}b^2 = a^2, \quad a^2c = ca^2,$$

т.е. a^2 содержится в центре группы G. Поскольку

$$ac = ca^{-1}b, \quad a^3c = a^2ca^{-1}b, \quad a^{-1}ca = a^2ca^{-1}ba = a^2cb = c \cdot ba^2,$$

то группа G разлагается в полупрямое произведение

$$G = (\langle c\rangle \times \left\langle ba^2\right\rangle) \leftthreetimes \langle a\rangle \cong (C_2 \times C_2) \leftthreetimes C_4.$$

Обозначим через x и y проекции группы G на ее подгруппы $\langle c\rangle$ и $\langle a\rangle$ соответственно. Тогда $x, y \in I(G)$ и

$$\begin{gathered}\operatorname{Im} x = \langle c\rangle, \quad \operatorname{Ker} x = \langle a\rangle \times \langle b\rangle, \quad \operatorname{Im} y = \langle a\rangle, \\ \operatorname{Ker} y = \langle c\rangle \times \left\langle ba^2\right\rangle, \quad \operatorname{Ker} x \cap \operatorname{Ker} y = \left\langle ba^2\right\rangle.\end{gathered} \tag{4.2}$$

Докажем теперь некоторые свойства идемпотентов x и y в полугруппе $\operatorname{End}(G)$.

Лемма 4.1. *Идемпотенты x и y удовлетворяют условиям*

$$K(x) \cong \operatorname{End}(C_2), \quad K(y) \cong \operatorname{End}(C_4), \tag{4.3}$$

$$xy = yx = 0, \tag{4.4}$$

$$I(G) \cap J(x) \cap J(y) = \{0\}. \tag{4.5}$$

Доказательство. Изоморфизмы (4.3) вытекают непосредственно из леммы 2.9. Так как $\operatorname{Im} x \subset \operatorname{Ker} y$ и $\operatorname{Im} y \subset \operatorname{Ker} x$, то $xy = yx = 0$ и, следовательно, справедливы равенства (4.4). Предположим, что $z \in I(G) \cap J(x) \cap J(y) = \{0\}$. Тогда $xz = yz = 0$ и $cz = az = 1$. Поскольку $c^{-1}ac = a^{-1}b$, то

$$1 = (c^{-1}ac)z = (a^{-1}b)z = bz,$$

т.е. $z = 0$. Следовательно, справедливо равенство (4.5). Лемма доказана. □

Лемма 4.2. *Подгруппа $V(x) \cap V(y)$ группы $\operatorname{Aut}(G)$ является 2-группой.*

Доказательство. Определим элементы подгруппы $V(x) \cap V(y)$. Предположим, что $z \in V(x) \cap V(y)$. Тогда $zx = x$, $zy = y$, и $g^{-1} \cdot gz \in \operatorname{Ker} x \cap \operatorname{Ker} y$ для каждого $g \in G$. Следовательно,

$$z : \begin{cases} c \mapsto cb^i a^{2i}, \\ a \mapsto ab^j a^{2j}, \\ b \mapsto bb^k a^{2k} \end{cases} \tag{4.6}$$

для некоторых $i, j, k \in \{0, 1\}$. Отображение (4.6) сохраняет определяющие соотношения группы (4.1) группы G тогда и только тогда, когда оно сохраняет соотношение $c^{-1}ac = a^{-1}b$, т.е.

$$\begin{gathered} (cz)^{-1}(az)(cz) = (az)^{-1}(bz), \\ a^{-2i}b^{-i}c^{-1}ab^j a^{2j}cb^i a^{2i} = a^{-2j}b^{-j}a^{-1}bb^k a^{2k}. \end{gathered} \tag{4.7}$$

Равенство (4.7) справедливо только при $k = 0$. Следовательно, подгруппа $V(x) \cap V(y)$ группы $\operatorname{Aut}(G)$ состоит из отображений (4.6), где $k = 0$ и $i, j \in \{0, 1\}$. Поэтому $|V(x) \cap V(y)| = 4$ и $V(x) \cap V(y)$ является 2-группой. Лемма доказана. □

Лемма 4.3. *Идемпотенты x и y удовлетворяют равенству*

$$|J(x) \cap H(y)| = 2. \tag{4.8}$$

Доказательство. Пусть $z \in J(x) \cap H(y)$. Тогда $xz = zx = 0$, $yz = z$, $zy = 0$. Поэтому

$$\begin{gathered} (\operatorname{Im} x)z = \{1\}, \quad (\operatorname{Ker} x)z \subset \operatorname{Ker} x, \quad (\operatorname{Ker} y)z = \{1\}, \quad (\operatorname{Im} y)z \subset \operatorname{Ker} y, \\ cz = 1, \quad (\langle a \rangle \times \langle b \rangle)z \subset \langle a \rangle \times \langle b \rangle, \quad (ba^2)z = 1, \quad az \in \langle c \rangle \times \langle ba^2 \rangle. \end{gathered}$$

Отсюда вытекает, что

$$az \in \langle ba^2 \rangle, \quad a^2 z = 1, \quad (ba^2)z = bz = 1$$

и $az = (ba^2)^i$ для некоторого $i \in \{0, 1\}$. Следовательно,

$$z : \begin{cases} c \mapsto 1, \\ a \mapsto (ba^2)^i, \\ b \mapsto 1, \end{cases} \tag{4.9}$$

где $i \in \{0, 1\}$.

Наоборот, отображение (4.9) сохраняет при $i \in \{0, 1\}$ определяющие соотношения (4.1) группы G и является эндоморфизмом группы G. Легко проверить, что $z \in J(x) \cap H(y)$. Следовательно, выполняется равенство (4.8). Лемма доказана. □

Оказывается, что свойства полугруппы $\operatorname{End}(G)$, представленные в леммах 4.1–4.3, характерны только для группы G. Для доказательства этого факта выберем произвольную группу G^*, полугруппа эндоморфизмов которой изоморфна полугруппе $\operatorname{End}(G)$:

$$\operatorname{End}(G) \cong \operatorname{End}(G^*). \tag{4.10}$$

Мы докажем, что в таком случае группы G и G^* тоже изоморфны. Обозначим в дальнейшем через z^* образ элемента $z \in \operatorname{End}(G)$ в изоморфизме (4.10). Отметим, что ввиду конечности полугруппы $\operatorname{End}(G^*)$ группа G^* также конечна [3, теорема 2].

В леммах 4.1–4.3 доказаны некоторые свойства идемпотентов $x, y \in I(G)$. В силу изоморфизма (4.10) идемпотенты x^* и y^* полугруппы $\mathrm{End}(G^*)$ удовлетворяют аналогичным свойствам в полугруппе $\mathrm{End}(G^*)$. Следовательно, x^* и y^* обладают следующими свойствами:

(1^*) $K(x^*) \cong \mathrm{End}(C_2)$;
(2^*) $K(y^*) \cong (C_4)$;
(3^*) $x^*y^* = y^*x^* = 0^*$;
(4^*) $I(G^*) \cap J(x^*) \cap J(y^*) = \{0^*\}$;
(5^*) $V(x^*) \cap V(y^*)$ является 2-группой;
(6^*) $|J(x^*) \cap H(y^*)| = 2$.

Из леммы 2.9 и свойства (1^*) вытекает изоморфизм $\mathrm{End}(\mathrm{Im}\, x^*) \cong \mathrm{End}(C_2)$. Так как каждая конечная абелева группа определяется своей полугруппой эндоморфизмов, то $\mathrm{Im}\, x^* \cong C_2$. Аналогично, по свойству (2^*), $\mathrm{Im}\, y^* \cong C_4$. Поэтому существуют такие $c, a \in G^*$, что

$$\mathrm{Im}\, x^* = \langle c \rangle \cong C_2, \quad \mathrm{Im}\, y^* = \langle a \rangle \cong C_4$$

(здесь a и c не являются порождающими элементами группы G).

Ввиду свойства (3^*),

$$(\mathrm{Im}\, x^*)y^* = \{1\}, \quad (\mathrm{Ker}\, x^*)y^* \subset \mathrm{Ker}\, x^*, \quad (\mathrm{Im}\, y^*)x^* = \{1\}, \quad (\mathrm{Ker}\, y^*)x^* \subset \mathrm{Ker}\, y^*,$$

откуда согласно леммам 2.6 и 2.8

$$G^* = ((\mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*) \leftthreetimes \mathrm{Im}\, y^*) \leftthreetimes \mathrm{Im}\, x^* = ((\mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*) \leftthreetimes \mathrm{Im}\, x^*) \leftthreetimes \mathrm{Im}\, y^*.$$

Пусть

$$N = \mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*.$$

Тогда

$$G^* = (N \leftthreetimes \langle a \rangle) \leftthreetimes \langle c \rangle = (N \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle . \tag{4.11}$$

Лемма 4.4. *Группа G^* является 2-группой.*

Доказательство. Так как группы $\mathrm{Im}\, x^*$ и $\mathrm{Im}\, y^*$ абелевы, то согласно лемме 2.7

$$\widehat{g} \in V(x^*) \cap V(y^*) \quad \text{для всех } g \in G^*. \tag{4.12}$$

В силу (4.12) и свойства (5^*) каждый $2'$-элемент группы G^* содержится в центре группы G^*. Поэтому

$$G^* = G_2^* \times G_{2'}^*, \quad G_{2'}^* \subset N,$$
$$G_2^* = ((N \cap G_2^*) \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle = ((N \cap G_2^*) \leftthreetimes \langle a \rangle) \leftthreetimes \langle c \rangle ,$$

где G_2^* и $G_{2'}^*$ обозначают соответственно силовскую 2-подгруппу и холловскую $2'$-подгруппу группы G^*.

Обозначим через z^* проекцию группы G^* на ее подгруппу $G_{2'}^*$. Ясно, что $z^* \in I(G^*) \cap J(x^*) \cap J(y^*)$. По свойству (4^*), $z^* = 0^*$, т.е. $G_{2'}^* = \{1\}$ и G^* является 2-группой. Лемма доказана. □

Лемма 4.5. $N \cong C_2$.

Доказательство. Предположим, что $z^* \in J(x^*) \cap H(y^*)$. Тогда

$$z^*x^* = x^*z^* = 0^*, \quad y^*z^* = z^*, \quad z^*y^* = 0^*,$$
$$\mathrm{Im}\, z^* \subset \mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^* = N, \quad \mathrm{Ker}\, y^* \subset \mathrm{Ker}\, z^*.$$

Поэтому эндоморфизм z^* разлагается в произведение $z^* = y^* \cdot \varphi$, где $\varphi : \mathrm{Im}\, y^* \to N$ является ограничением эндоморфизма z^* на подгруппу $\mathrm{Im}\, y^* = \langle a \rangle$. Наоборот, если выбрать некоторый гомоморфизм $\varphi : \mathrm{Im}\, y^* = \langle a \rangle \to N$, то $y^* \cdot \varphi \in J(x^*) \cap H(y^*)$. Следовательно,

$$|J(x^*) \cap H(y^*)| = |\,\mathrm{Hom}(\langle a \rangle , N)| = 2. \tag{4.13}$$

Из равенства (4.13) вытекает, что подгруппа N группы G^* содержит только один элемент второго порядка. Согласно [12, теорема 5.3.6] группа N является циклической группой или обобщенной группой кватернионов. Так как $\langle a\rangle \cong C_4$ и обобщенная группа кватернионов содержит элемент четвертого порядка, то группа N является циклической группой второго порядка. Лемма доказана. □

Обозначим образующий элемент группы N через d:

$$N = \langle d\rangle \cong C_2.$$

Ясно, что d содержится в центре группы G^*, т.е.

$$gd = dg \quad \forall g \in G^*.$$

Если $ac = ca$, то в силу (4.11)

$$G^* = N \times \langle a\rangle \times \langle c\rangle$$

и $z^* \in I(G^*) \cap J(x^*) \cap J(y^*)$, $z^* \neq 0^*$ где z^* является проекцией группы G^* на ее подгруппу N. Это противоречит свойству (4^*). Поэтому $ac \neq ca$ и $[a,c] = a^{-1}c^{-1}ac \neq 1$. Из равенств (4.11) следует теперь, что факторгруппа G^*/N абелева, т.е. $[a,c] \in N = \langle d\rangle$, $[a,c] = d$ и $c^{-1}ac = ad$ Следовательно,

$$c^{-1}a^2c = a^2d^2 = a^2, \quad a^2c = ca^2,$$

и a^2 содержится в центре группы G^*.

Обозначим $b = a^2d$ Тогда

$$b \in Z(G^*), \quad b^2 = 1, \quad c^{-1}ac = ad = aa^{-2}b = a^{-1}b,$$
$$\langle a, N\rangle = N \leftthreetimes \langle a\rangle = N \times \langle a\rangle = \langle d\rangle \times \langle a\rangle = \langle b\rangle \times \langle a\rangle$$

и

$$G^* = (\langle b\rangle \times \langle a\rangle) \leftthreetimes \langle c\rangle = \left\langle a, b, c \mid a^4 = b^2 = c^2 = 1, bc = cb, ab = ba, c^{-1}ac = a^{-1}b\right\rangle. \tag{4.14}$$

Из определяющих соотношений (4.1) группы G и определяющих соотношений (4.14) группы G^* вытекает изоморфизм групп G и G^*.

Следствие 4.1. *Пусть G^* — некоторая группа. Группа G^* изоморфна группе $\mathscr{G}_7$ тогда и только тогда, когда существуют такие $x^*, y^* \in I(G^*)$, которые удовлетворяют свойствам* (1^*)–(6^*).

Этим доказано, что группа $G = \mathscr{G}_7$ определяется своей полугруппой эндоморфизмов в классе всех групп.

5. Описание группы $\mathscr{G}_8$ ее полугруппой эндоморфизмов

В этом разделе докажем, что группа $\mathscr{G}_8$ определяется своей полугруппой эндоморфизмов в классе всех групп. Пусть всюду в этой главе $G = \mathscr{G}_8$. Согласно лемме 3.1

$$G = \langle a, b, c\rangle = (\langle a\rangle \times \langle c\rangle) \leftthreetimes \langle b\rangle \cong (C_4 \times C_2) \leftthreetimes C_2,$$

где

$$a^4 = b^2 = c^2 = 1, \quad ac = ca, \quad b^{-1}cb = ca^2, \quad b^{-1}ab = a^{-1}. \tag{5.1}$$

Из равенств (5.1) вытекает

$$b^{-1}a^2b = a^{-2} = a^2, \quad a^2b = ba^2,$$

т.е. a^2 содержится в центре группы G. Так как

$$c^{-1}bc = c^{-1}b^{-1}c = a^2b^{-1} = a^2b = ba^2,$$

то G разлагается в полупрямое произведение

$$G = (\langle a\rangle \leftthreetimes \langle b\rangle) \leftthreetimes \langle c\rangle \cong (C_4 \leftthreetimes C_2) \leftthreetimes C_2.$$

Обозначим соответственно через x и y проекции группы G на ее подгруппы $\langle b\rangle$ и $\langle c\rangle$. Тогда $x, y \in I(G)$ и

$$\operatorname{Im} x = \langle b\rangle, \quad \operatorname{Ker} x = \langle a\rangle \times \langle c\rangle, \quad \operatorname{Im} y = \langle c\rangle, \quad \operatorname{Ker} y = \langle a\rangle \leftthreetimes \langle b\rangle, \quad \operatorname{Ker} x \cap \operatorname{Ker} y = \langle a\rangle. \tag{5.2}$$

Докажем некоторые свойства идемпотентов x и y полугруппы $\operatorname{End}(G)$.

Лемма 5.1. *Идемпотенты x и y удовлетворяют условиям*

$$K(x) \cong \operatorname{End}(C_2), \quad K(y) \cong \operatorname{End}(C_2), \tag{5.3}$$

$$xy = yx = 0, \tag{5.4}$$

$$I(G) \cap J(x) \cap J(y) = \{0\}, \tag{5.5}$$

$$|J(x) \cap J(y)| = 2, \tag{5.6}$$

$$z^2 = 0 \quad \forall z \in J(x) \cap J(y). \tag{5.7}$$

Доказательство. Изоморфизмы (5.3) следуют непосредственно из леммы 2.9. Так как $\operatorname{Im} x \subset \operatorname{Ker} y$ и $\operatorname{Im} y \subset \operatorname{Ker} x$, то $xy = yx = 0$ и справедливы равенства (5.4).

Предположим, что $z \in J(x) \cap J(y) = \{0\}$. Тогда $xz = zx = yz = zy = 0$ и

$$cz = bz = 1, \quad (\operatorname{Ker} x \cap \operatorname{Ker} y)z \subset \operatorname{Ker} x \cap \operatorname{Ker} y.$$

Поэтому из (5.2) вытекает, что $az = a^i$ для некоторого i. Применяя эндоморфизм z к равенству $b^{-1}cb = ca^2$, получим $1 = (az)^2 = a^{2i}$, т.е. $i \in \{0, 1\}$. Следовательно,

$$z : \begin{cases} b \mapsto 1, \\ c \mapsto 1, \\ a \mapsto a^{2i}, \end{cases} \tag{5.8}$$

где $i \in \{0, 1\}$. Наоборот, каждое отображение z, заданное при помощи (5.8), сохраняет определяющие соотношения (5.1) группы G и поэтому расширяется до эндоморфизма группы G. Ясно, что полученный эндоморфизм принадлежит к $J(x) \cap J(y)$ и $z^2 = 0$. Отображение (5.8) является идемпотентом тогда и только тогда, когда $i = 0$, т.е. $z = 0$. Следовательно, все условия (5.5)–(5.7) выполняются. Лемма доказана. □

Лемма 5.2. *Подгруппа $V(x) \cap V(y)$ группы $\operatorname{Aut}(G)$ является 2-группой.*

Доказательство. Найдем элементы группы $V(x) \cap V(y)$. Пусть $z \in V(x) \cap V(y)$. Тогда $zx = x$, $zy = y$ и $g^{-1} \cdot gz \in \operatorname{Ker} x \cap \operatorname{Ker} y$ для каждого $g \in G$. Поэтому

$$z : \begin{cases} b \mapsto ba^i, \\ c \mapsto ca^j, \\ a \mapsto a^k \end{cases} \tag{5.9}$$

для некоторых $i, j, k \in \{0, 1, 2, 3\}$. Легко проверить, что отображение (5.9) сохраняет определяющие соотношения (5.1) группы G тогда и только тогда, когда

$$i \in \{0, 1, 2, 3\}, \quad j \in \{0, 2\}, \quad k \in \{1, 3\}. \tag{5.10}$$

Наоборот, если выбрать числа i, j, k так, как указано в (5.10), то отображение (5.9) удовлетворяет равенству $\langle a, b, c\rangle = \langle az, bz, cz\rangle$ и, следовательно, является автоморфизмом группы G. Простые вычисления показывают, что $zx = x$ и $zy = y$, т.е. $z \in V(x) \cap V(y)$. Количество троек (i, j, k), удовлетворяющих условиям (5.10), равно 16. Поэтому $|V(x) \cap V(y)| = 16$ и $V(x) \cap V(y)$ является 2-группой. Лемма доказана. □

Лемма 5.3. *Если $z \in J(x) \cap J(y)$, $z \neq 0$, то*

$$\big|\{u \in [x] \mid uz = 0\}\big| = 2. \tag{5.11}$$

Доказательство. Найдем сначала элементы множества $[x]$. В силу (5.2) и леммы 2.10 множество $[x]$ состоит из эндоморфизмов y группы G, которые имеют вид

$$u : \begin{cases} b \mapsto bc^i a^j, \\ c \mapsto 1, \\ a \mapsto 1. \end{cases} \tag{5.12}$$

Отображение y, заданное условиями (5.12), сохраняет определяющие соотношения группы G и является эндоморфизмом группы G тогда и только тогда, когда $i = 0$. Поэтому множество $[x]$ состоит из отображений

$$u : \begin{cases} b \mapsto ba^j, \\ c \mapsto 1, \\ a \mapsto 1, \end{cases} \qquad j \in \{0, 1, 2, 3\}. \tag{5.13}$$

Предположим, что $z \in J(x) \cap J(y)$, $z \neq 0$. В лемме 5.2 доказано, что

$$z : \begin{cases} b \mapsto 1, \\ c \mapsto 1, \\ a \mapsto a^2. \end{cases} \tag{5.14}$$

Произведение uz отображений (5.13) и (5.14) равно

$$uz : \begin{cases} b \mapsto a^{2j}, \\ c \mapsto 1, \\ a \mapsto 1, \end{cases}$$

и $uz = 0$ тогда и только тогда, когда $j \in \{0, 2\}$. Следовательно, справедливо равенство (5.11). Лемма доказана. □

Так как множество $[x]$ состоит из отображений (5.13), то

$$\big|[x]\big| = 4.$$

Произведение uz равно нулю для каждого $u \in [x]$, т.е. $[x] \cdot y = \{0\}$

Лемма 5.4. *Идемпотент y удовлетворяет равенству*

$$\big|[y]\big| = 2. \tag{5.15}$$

Доказательство. Аналогично лемме 5.3 можно проверить, что множество $[y]$ состоит из двух отображений

$$y : \begin{cases} b \mapsto 1, \\ c \mapsto c, \\ a \mapsto 1, \end{cases} \qquad w : \begin{cases} b \mapsto 1, \\ c \mapsto ca^2, \\ a \mapsto 1. \end{cases}$$

Лемма доказана. □

Оказывается, что доказанные здесь свойства полугруппы $\mathrm{End}(G)$ характерны только для группы G. Для доказательства этого факта выберем произвольную группу G^*, полугруппа эндоморфизмов которой изоморфна полугруппе $\mathrm{End}(G^*)$:

$$\mathrm{End}(G) \cong \mathrm{End}(G^*). \tag{5.16}$$

Мы докажем, что в таком случае группы G и G^* тоже изоморфны. Обозначим в дальнейшем через z^* образ элемента $z \in \mathrm{End}(G)$ в изоморфизме (5.16). Отметим, что ввиду конечности полугруппы $\mathrm{End}(G^*)$ группа G^* также конечна [3, теорема 2].

В леммах 5.1–5.4 доказаны некоторые свойства идемпотентов $x, y \in I(G)$. В силу изоморфизма (5.16) идемпотенты x^* и y^* полугруппы $\mathrm{End}(G^*)$ удовлетворяют аналогичным свойствам в полугруппе $\mathrm{End}(G^*)$. Следовательно, x^* и y^* обладают следующими свойствами:

(1*) $K(x^*) \cong \mathrm{End}(C_2)$;
(2*) $K(y^*) \cong \mathrm{End}(C_2)$;
(3*) $x^*y^* = y^*x^* = 0^*$;
(4*) $I(G^*) \cap J(x^*) \cap J(y^*) = \{0^*\}$;
(5*) $V(x^*) \cap V(y^*)$ является 2-группой;
(6*) $|J(x^*) \cap J(y^*)| = 2$ и $(z^*)^2 = 0^*$ для каждого $z^* \in J(x^*) \cap J(y^*)$;
(7*) Если $z^* \in J(x^*) \cap J(y^*)$, $z^* \neq 0^*$, то $\left|\{u^* \in [x^*] \mid u^*z^* = 0^*\}\right| = 2$;
(8*) $\left|[y^*]\right| = 2$;
(9*) $\left|[x^*]\right| = 4$;
(10*) $[x^*] \cdot y^* = \{0^*\}$.

Из леммы 2.9, вытекает, что

$$K(x^*) \cong \mathrm{End}(\mathrm{Im}\, x^*), \quad K(y^*) \cong \mathrm{End}(\mathrm{Im}\, y^*).$$

Согласно лемме 2.1 и свойству (1*) имеем $\mathrm{Im}\, x^* \cong C_2$. Аналогично, $\mathrm{Im}\, y^* \cong C_2$. Поэтому существуют такие $b, c \in G^*$ что

$$\mathrm{Im}\, x^* = \langle b \rangle \cong C_2, \quad \mathrm{Im}\, y^* = \langle c \rangle \cong C_2.$$

Из свойства (3*) следует, что

$$(\mathrm{Im}\, x^*)y^* = \{1\}, \quad (\mathrm{Ker}\, x^*)y^* \subset \mathrm{Ker}\, x^*, \quad (\mathrm{Im}\, y^*)x^* = \{1\}, \quad (\mathrm{Ker}\, y^*)x^* \subset \mathrm{Ker}\, y^*.$$

Следовательно,

$$G^* = ((\mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*) \leftthreetimes \mathrm{Im}\, y^*) \leftthreetimes \mathrm{Im}\, x^* = ((\mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*) \leftthreetimes \mathrm{Im}\, x^*) \leftthreetimes \mathrm{Im}\, y^*.$$

Обозначим $N = \mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*$ Тогда

$$G^* = (N \leftthreetimes \langle c \rangle) \leftthreetimes \langle b \rangle = (N \leftthreetimes \langle b \rangle) \leftthreetimes \langle c \rangle. \tag{5.17}$$

Лемма 5.5. *Группа G^* является 2-группой и ее подгруппа N является циклической или обобщенной группой кватернионов.*

Доказательство. Поскольку группы $\mathrm{Im}\, x^*$ и $\mathrm{Im}\, y^*$ абелевы, то согласно лемме 2.7

$$\widehat{g} \in V(x^*) \cap V(y^*) \quad \forall g \in G^*. \tag{5.18}$$

Ввиду условия (5.18) и свойства (5*) все $2'$-элементы группы G^* содержатся в центре группы G^*. Поэтому

$$G^* = G_2^* \times G_{2'}^*, \quad G_{2'}^* \subset N,$$
$$G_2^* = ((N \cap G_2^*) \leftthreetimes \langle c \rangle) \leftthreetimes \langle b \rangle = ((N \cap G_2^*) \leftthreetimes \langle b \rangle) \leftthreetimes \langle c \rangle,$$

где G_2^* и $G_{2'}^*$ обозначают соответственно силовскую 2-подгруппу и холловскую $2'$-подгруппу группы G^*.

Обозначим через z^* проекцию группы G^* на ее подгруппу $G_{2'}^*$. Тогда $z^* \in I(G^*) \cap J(x^*) \cap J(y^*)$, откуда ввиду свойства (4*) получаем $z^* = 0^*$, т.е., $G_{2'}^* = \{1\}$ и G^* является 2-группой.

Предположим, что $z^* \in J(x^*) \cap J(y^*)$, $z^* \neq 0^*$ Тогда

$$z^*x^* = x^*z^* = z^*y^* = y^*z^* = 0^*, \tag{5.19}$$
$$(\mathrm{Im}\, x^*)z^* = (\mathrm{Im}\, y^*)z^* = \{1\}, \tag{5.20}$$
$$(\mathrm{Ker}\, x^*)z^* \subset \mathrm{Ker}\, x^*, \quad (\mathrm{Ker}\, y^*)z^* \subset \mathrm{Ker}\, y^*, \tag{5.21}$$
$$\mathrm{Im}\, z^* = Nz^* = (\mathrm{Ker}\, x^* \cap \mathrm{Ker}\, y^*)z^* \subset N. \tag{5.22}$$

Выберем произвольный элемент $d \in N$ второго порядка. Так как $\mathrm{Im}\, z^*$ является конечной 2-группой, то существует гомоморфизм $\varphi_d : \mathrm{Im}\, z^* \to \langle d \rangle$, для которого $\mathrm{Im}\, \varphi_d = \langle d \rangle$. Произведение $z^* \cdot \varphi_d$ будет эндоморфизмом группы G^*. В силу построения и условий (5.19)–(5.22) ясно, что

$$z^* \cdot \varphi_d \in J(x^*) \cap J(y^*), \quad z^* \cdot \varphi_d \neq 0^*.$$

Согласно свойству (6^*) видим,что $J(x^*) \cap J(y^*)$ имеет только один ненулевой элемент. Поэтому группа N содержит только один элемент второго порядка и $z^* = z^* \cdot \varphi_d$. Следовательно, группа N циклична или является обобщенной группой кватернионов [12, теорема 5.3.6]. Лемма доказана. $\square$

Обозначим в дальнейшем через d единственный элемент второго порядка группы N и через z^* единственный ненулевой элемент множества $J(x^*) \cap J(y^*)$ Ясно, что d содержится в центре группы G^*. Введем также обозначение

$$N_0 = \operatorname{Ker} x^* \cap \operatorname{Ker} y^* \cap \operatorname{Ker} z^* = N \cap \operatorname{Ker} z^*.$$

Так как группы $\operatorname{Im} x^*$, $\operatorname{Im} y^*$ и $\operatorname{Im} z^*$ абелевы, то коммутант $(G^*)'$ группы G^* содержится в N_0:

$$(G^*)' \subset N_0. \tag{5.23}$$

Поэтому факторгруппа G^*/N_0 абелева и

$$G^*/N_0 = (N/N_0) \times \langle cN \rangle \times \langle bN \rangle \cong C_2 \times C_2 \times C_2. \tag{5.24}$$

Поскольку $(z^*)^2 = 0^*$, то $d \in N_0$.

Отображение

$$v^* : \begin{cases} b \mapsto bd, \\ c \mapsto 1, \\ h \mapsto 1, \quad h \in N, \end{cases}$$

можно расширить до эндоморфизма группы G^*. При этом $(v^*)^2 = v^*$, $x^*v^* = v^*$, $v^*x^* = x^*$, т.е. $v^* \in [x^*]$. Дополнительно имеем $v^* \neq x^*$, $v^*z^* = 0^*$, $x^*z^* = 0^*$. Следовательно, в силу свойства (7^*),

$$\{u^* \in [x^*] \mid u^*z^* = 0^*\} = \{x^*, v^*\}. \tag{5.25}$$

Рассмотрим теперь отображение

$$w^* : \begin{cases} b \mapsto 1, \\ c \mapsto cd, \\ h \mapsto 1, \quad h \in N. \end{cases}$$

Отображение w^* можно расширить до эндоморфизма группы G^*. Ясно, что $w^* \in [y^*]$. Так как $w^* \neq y^*$, то в силу свойства (8^*)

$$[y^*] = \{y^*, w^*\}. \tag{5.26}$$

Лемма 5.6. *Элементы b, c, d группы G^* удовлетворяют равенствам*

$$b^{-1}cb = cd, \quad c^{-1}bc = bd, \tag{5.27}$$

$$cg = gc \quad \textit{или} \quad [c, g] = d, \tag{5.28}$$

$$bg = gb \quad \textit{или} \quad [b, g] = d \tag{5.29}$$

для каждого $g \in G^*$

Доказательство. Пусть $g \in G^*$. Тогда $x^* \cdot \widehat{g} \in [x^*]$. Так как $\operatorname{Im} x^* = \langle b \rangle$ и $b\widehat{g} = b \cdot [b, g]$ то в силу (5.23) имеем $(x^* \cdot \widehat{g}) \cdot z^* = 0^*$. Из равенства (5.25) вытекает $x^* \cdot \widehat{g} \in \{x^*, v^*\}$ т.е. $[b, g] = 1$ или $[b, g] = d$. Поэтому справедливо условие (5.29). Аналогично, условие (5.28) вытекает из равенства (5.26) и включения $y^* \cdot \widehat{g} \in [y^*]$.

Предположим, что $bc = cb$. Тогда отображение

$$s^* : \begin{cases} b \mapsto 1, \\ c \mapsto cb, \\ h \mapsto 1, \quad h \in N, \end{cases}$$

можно расширить до эндоморфизма группы G^* и $s^* \in [y^*]$, $s^* \neq y^*$ Ввиду равенства (5.26) имеем $d = b$. Это противоречит выбору элементов d и b. Следовательно, $bc \neq cb$ и ввиду условия(5.28) $[c, b] = d$, т.е.

$$c^{-1}b^{-1}cb = d, \quad b^{-1}cb = cd, \quad c^{-1}b^{-1}c = db^{-1}, \quad c^{-1}bc = bd^{-1} = bd.$$

Лемма доказана. □

Положим $M = \langle b, c\rangle$. Из равенств (5.27) вытекает

$$M = \langle b, c\rangle = (\langle d\rangle \times \langle c\rangle) \leftthreetimes \langle b\rangle = (\langle d\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle .$$

Поскольку $d \in Z(G^*)$, $g^{-1}bg = b \cdot [b, g]$ и $g^{-1}cg = c \cdot [c, g]$, то в силу условий (5.28) и (5.29) группа M является нормальным делителем группы G^*. Ввиду равенств (5.17) получим изоморфизм

$$G^*/M \cong N/\langle d\rangle .$$

Лемма 5.7. *Подгруппа N группы G^* является циклической группой порядка 4.*

Доказательство. В лемме 5.5 было доказано, что группа N является циклической 2-группой или обобщенной группой кватернионов. Предположим, что группа N является обобщенной группой кватернионов Q_n, $n \geqslant 2$:

$$Q_n = \left\langle a_0, b_0 \;\middle|\; {a_0}^{2^n} = 1,\ {b_0}^2 = {a_0}^{2^{n-1}},\ {b_0}^{-1}a_0b_0 = {a_0}^{-1} \right\rangle .$$

Поскольку $Z(Q_n) = \left\langle {a_0}^{2^{n-1}} \right\rangle \cong C_2$ и $d \in Z(N)$, то $d = {a_0}^{2^{n-1}}$. Обозначим $S = \left\langle {a_0}^2 \right\rangle$. Тогда

$$N/S = \langle a_0S\rangle \times \langle b_0S\rangle \cong C_2 \times C_2.$$

Так как $d \in S$, то возникает естественный гомоморфизм

$$\varphi : N/\langle d\rangle \to N/S, \quad (g \cdot \langle d\rangle)\varphi = gS \quad (g \in N).$$

Рассмотрим эндоморфизмы τ и μ группы G^*, являющиеся произведениями следующих гомоморфизмов:

$$G^* \xrightarrow{\pi} G^*/M \cong N/\langle d\rangle \xrightarrow{\varphi} N/S \xrightarrow{\pi_1} \langle a_0S\rangle \xrightarrow{\alpha} \langle d\rangle ,$$

$$G^* \xrightarrow{\pi} G^*/M \cong N/\langle d\rangle \xrightarrow{\varphi} N/S \xrightarrow{\pi_2} \langle a_0S\rangle \xrightarrow{\beta} \langle d\rangle ,$$

где π — естественный гомоморфизм, π_1 и π_2 — проекции группы N/S на ее подгруппы $\langle a_0S\rangle$ и $\langle b_0S\rangle$ соответственно и $(a_0S)\alpha = (b_0S)\beta = d$. По построению $\tau \neq 0^*$, $\mu \neq 0^*$, $\tau \neq \mu$ и $\tau, \mu \in J(x^*) \cap J(y^*)$. Это противоречит свойству (6^*), так как $0^* \in J(x^*) \cap J(y^*)$. Следовательно, группа N не может быть обобщенной группой кватернионов. Таким образом, группа N циклична.

Предположим, что $N = \langle a\rangle \cong C_{2^n}$ Ранее было доказано, что $n \geqslant 2$ (см. (5.23)). Так как d является единственным элементом второго порядка в группе N, то $d = a^{2^{n-1}}$

Обозначим через σ_i эндоморфизм группы G^*, являющийся произведением следующих гомоморфизмов:

$$G^* \xrightarrow{\pi} G^*/M \cong N/\langle d\rangle = \langle a\rangle/\langle a^{2^{n-1}}\rangle \xrightarrow{\gamma} \left\langle a^{2i}\right\rangle ,$$

где π — естественный гомоморфизм и

$$(a/\langle a^{2^{n-1}}\rangle)\gamma = a^{2i}, \quad i \in \{0, 1, \ldots, 2^{n-1} - 1\}.$$

По построению ясно, что $\sigma_i \in J(x^*) \cap J(y^*)$. В силу свойства (6^*) число i может принимать только два различных значения. Следовательно, $n = 2$ и $N = \langle a\rangle \cong C_4$. Лемма доказана. □

Уже доказано, что

$$N = \langle a\rangle \cong C_4, \quad d = a^2.$$

Ввиду (5.17) и (5.27) имеем

$$G^* = (\langle a\rangle \leftthreetimes \langle b\rangle) \leftthreetimes \langle c\rangle = (\langle a\rangle \leftthreetimes \langle c\rangle) \leftthreetimes \langle b\rangle , \quad b^{-1}cb = ca^2, \quad c^{-1}bc = ba^2. \tag{5.30}$$

Лемма 5.8. *Порождающие элементы a, b, c группы G^* удовлетворяют равенствам*

$$ac = ca, \quad b^{-1}ab = a^{-1}. \tag{5.31}$$

Доказательство. Ввиду (5.28) имеем $ca = ac$ или $[c, a] = d = a^2$. Рассмотрим сначала случай $[c, a] = a^2$. В таком случае

$$c^{-1}a^{-1}ca = a^2, \quad c^{-1}a^{-1}c = a, \quad c^{-1}ac = a^{-1},$$
$$(ca^{-1})^2 = ca^{-1} \cdot ca^{-1} = (c^{-1}ac)^{-1} \cdot a^{-1} = a \cdot a^{-1} = 1,$$

поэтому отображение

$$s^* : \begin{cases} b \mapsto 1, \\ c \mapsto ca^{-1}, \\ a \mapsto 1 \end{cases}$$

можно расширить до эндоморфизма группы G^*. Дополнительно имеем $s^* \in [y^*]$, $s^* \neq y^*$. В силу (5.26) имеем $s^* = w^*$, т.е. $ca^{-1} = cd$, $a^{-1} = d = a^2$, $a^3 = 1$, что невозможно. Следовательно, $ac = ca$.

Согласно свойству (9^*) множество $[x^*]$ состоит из четырех элементов. Ввиду свойства (10^*) каждый $s^* \in [x^*]$ имеет вид

$$s^* : \begin{cases} b \mapsto ba^i, \\ c \mapsto 1, \\ a \mapsto 1, \end{cases} \tag{5.32}$$

где $i \in \{0, 1, 2, 3\}$. Так как $|[x^*]| = 4$, то отображение (5.32) можно расширить до эндоморфизма группы G^* для каждого $i \in \{0, 1, 2, 3\}$. При выполнении условия $ab = ba$ это невозможно, ибо тогда порядок элемента b равняется 2, но порядок элемента ba равняется 4. Следовательно, $ab \neq ba$. Условие (5.29) дает теперь равенства $[b, a] = d = a^2$ и

$$b^{-1}a^{-1}ba = a^2, \quad b^{-1}a^{-1}b = a, \quad b^{-1}ab = a^{-1}.$$

Лемма доказана. □

Легко проверить, что равенства (5.30) равносильны. Все полученные выше соотношения для порождающих a, b и c группы G^* дают

$$G^* = \left\langle a, b, c \;\middle|\; a^4 = b^2 = c^2 = 1,\ ac = ca,\ b^{-1}cb = ca^2,\ b^{-1}ab = a^{-1} \right\rangle.$$

Из последнего равенства и равенств (5.1) вытекает, что группы G и G^* изоморфны.

Следствие 5.1. *Пусть G^* — некоторая группа. Группа G^* изоморфна группе $\mathscr{G}_8$ тогда и только тогда, когда существуют такие $x^*, y^* \in I(G^*)$, которые удовлетворяют свойствам* (1^*)–(10^*).

Этим доказано, что группа $G = \mathscr{G}_8$ определяется своей полугруппой эндоморфизмов в классе всех групп. Это завершает также доказательство теоремы, сформулированной во введении настоящей статьи, т.е. доказано, что каждая группа порядка 16 определяется своей полугруппой эндоморфизмов в классе всех групп.

СПИСОК ЛИТЕРАТУРЫ

1. *Пуусемп П.* Идемпотенты полугрупп эндоморфизмов групп// Acta Comment. Univ. Tartuensis. — 1975. — *366*. — С. 76–104.
2. *Пуусемп П.* Полугруппы эндоморфизмов обобщенных кватернионных групп// Acta Comment. Univ. Tartuensis. — 1976. — *390*. — С. 84–103.
3. *Alperin J. L.* Groups with finitely many automorphisms// Pac. J. Math. — 1962. — *12*, № 1. — С. 1–5.
4. *Corner A. L. S.* Every countable reduced torsion-free ring is an endomorphism ring// Proc. London Math. Soc. — 1963. — *13*. — С. 687–710.

5. *Coxeter H. S. M., Moser W. O. J.* Generators and relations for discrete groups. — Springer-Verlag, 1972.
6. *Puusemp P.* On the torsion subgroups and endomorphism semigroups of Abelian groups// Algebras Groups Geom. — 1997. — *14*. — С. 407–422.
7. *Puusemp P.* A characterization of divisible and torsion Abelian groups by their endomorphism semigroups// Algebras Groups Geom. — 1999. — *16*. — С. 183–193.
8. *Puusemp P.* On endomorphism semigroups of dihedral 2-groups and alternating group A_4// Algebras Groups Geom. — 1999. — *16*. — С. 487–500.
9. *Puusemp P.* Characterization of a semidirect product of cyclic groups by its endomorphism semigroup// Algebras Groups Geom. — 2000. — *17*. — С. 479–498.
10. *Puusemp P.* Characterization of a semidirect product of groups by its endomorphism semigroup// In: Proc. Int. Conf. Semigroups. Braga, Portugal, June 18–23, 1999/ P. Smith et al., eds. — Singapore: World Scientific, 2000. — С. 161–170.
11. *Puusemp P.* On the definability of a semidirect product of cyclic groups by its endomorphism semigroup// Algebras Groups Geom. — 2002. — *19*. — С. 195–212.
12. *Robinson D. J. S.* A course in the group theory/ Grad. Texts Math. — 1995. — *80*.

П. Пуусемп
Институт математики, Таллиннский технический университет
E-mail: puusemp@edu.ttu.ee

Современная математика и ее приложения. Том 14 (2004). С. 100–107

УДК 517.982

МУЛЬТИПЛИКАТИВНЫЕ СПЕКТРЫ БАНАХОВЫХ ПРОСТРАНСТВ

© 2004 г. **С. А. ШКАРИН, Ю. Н. КУЗНЕЦОВА**

Аннотация. Мультипликативным спектром комплексного банахова пространства X называется класс $\mathscr{K}(X)$ всех (автоматически компактных хаусдорфовых) топологических пространств, являющихся спектрами банаховых алгебр $(X,*)$ при задании на X всевозможных умножений, превращающих X в коммутативную ассоциативную комплексную алгебру с единицей. Изучаются свойства мультипликативных спектров. В частности, показано, что для всякого сепарабельного наследственно неразложимого пространства X класс $\mathscr{K}(X^n)$ состоит из счетных компактных пространств, имеющих не более n неизолированнных точек. Доказывается, что класс $\mathscr{K}(C[0,1])$ совпадает с классом всех метризуемых компактных пространств.

СОДЕРЖАНИЕ

1. Введение

Все банаховы пространства рассматриваются над полем комплескных чисел $\mathbb{C}$. Пусть X — банахово пространство. Тогда X' обозначает сопряженное пространство (пространство линейных непрерывных функционалов на X), а $\mathscr{M}(X)$ обозначает множество всех непрерывных умножений $*: X^2 \to X$, обращающих X в коммутативную ассоциативную алгебру с единицей. Для некоторого умножения $* \in \mathscr{M}(X)$ спектр $(X,*)$ (т.е. множество ненулевых характеров $\varkappa: X \to \mathbb{C}$) обозначается через $\Omega(X,*)$. Известно [6], что $\Omega(X,*)$ является $*$-слабо компактным подмножеством X'. (Напомним, что $*$-слабая топология — это топология на X', согласованная с двойственностью (X',X). Мы всегда предполагаем, что $\Omega(X,*)$ наделено $*$-слабой топологией.) Пусть $\mathscr{K}(X)$ обозначает класс всех (компактных хаусдорфовых) топологических пространств K, для которых существует такое умножение $* \in \mathscr{M}(X)$, что пространство $\Omega(X,*)$ гомеоморфно K. $\mathscr{K}(X)$ называется *мультипликативным спектром* банахова пространства X.

В настоящей работе изучены некоторые свойства мультипликативных спектров и найдены классы $\mathscr{K}(X)$ для некоторых банаховых пространств. Показано, в частности, что отображение $X \mapsto \mathscr{K}(X)$, определенное на бесконечномерных сепарабельных пространствах X, принимает бесконечно много различных значений. Таким образом, понятие мультипликативного спектра дает нетривиальную классификацию сепарабельных банаховых пространств. Наша основная цель — привлечь внимание к этой классификации.

2. Определения и обозначения

Как обычно, $\mathbb{R}$ и $\mathbb{Z}$ обозначают соответственно множества вещественных и целых чисел, $\mathbb{N} = \{n \in \mathbb{Z} : n \geqslant 1\}$, $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$, а $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$ обозначает одномерный тор. Для произвольного $n \in \mathbb{N}$ символ $\mathscr{S}_n$ обозначает класс счетных (включая конечные) хаусдорфовых компактных топологических пространств, имеющих не более n неизолированных точек, $\mathscr{S}_\omega$ обозначает

ISSN 1512–1712

класс счетных хаусдорфовых компактных топологических пространств, а $\mathscr{S}_{\mathrm{me}}$ обозначает класс метризуемых компактных пространств. Далее, $\mathscr{S}_{\mathrm{mag}}$ обозначает класс метризуемых компактных топологических пространств K, которые с помощью некоторого непрерывного умножения могут быть превращены в абелеву топологическую группу.

Пусть $\mathscr{K}_1, \mathscr{K}_2, \ldots$ — конечное или счетное множество классов компактных топологических пространств. Определим классы

$$\prod \mathscr{K}_j = \left\{ \prod K_j : K_j \in \mathscr{K}_j \right\}, \quad \mathscr{K} = \sum \mathscr{K}_j = \left\{ \sum K_j : K_j \in \mathscr{K}_j \right\}$$

и скажем, что классы $\prod \mathscr{K}_j$ и $\sum \mathscr{K}_j$ являются произведением и суммой классов $\mathscr{K}_j$ соответственно; здесь $\prod K_j$ обозначает тихоновское произведение пространств K_j, а $\sum K_j$ — дизъюнктное открыто-замкнутое объединение в случае конечного числа K_j и александровская компактификация [9] дизъюнктного открыто-замкнутого объединения, если число пространств K_j бесконечно.

Пусть K — топологическое пространство. *Простым склеиванием* называется факторпространство пространства K по отношению к следующему отношению эквивалентности: все классы, кроме одного, являются одноэлементными множествами, а один класс состоит из двух элементов. Скажем, что пространство L получено из пространства K *конечным склеиванием*, если оно гомеоморфно результату конечного числа простых склеиваний K.

Обозначим через $X_1 \widehat{\otimes} \ldots \widehat{\otimes} X_n$ пополнение тензорного произведения банаховых пространств X_j по проективной норме [6, 8], а через $L(X_1, X_2)$ — пространство линейных непрерывных операторов $T : X_1 \to X_2$. Напомним, что банахово пространство X называется *наследственно неразложимым*, если X бесконечномерно и для любых двух бесконечномерных замкнутых линейных подпространств Y и Z таких, что $Y \cap Z = \{0\}$, их сумма $Y + Z$ незамкнута в X. В [10] построены примеры сепарабельных (рефлексивных и нерефлексивных) наследственно неразложимых банаховых пространств.

3. Элементарные свойства мультипликативных спектров

Предложение 1. *Пусть X — банахово пространство, а Y — дополняемое подпространство X. Тогда $\mathscr{K}(Y) \subset \mathscr{K}(X)$.*

Доказательство. Пусть P — линейная непрерывная проекция X на Y, $* \in \mathscr{M}(Y)$, $e \in Y$ обозначает единицу в $(Y, *)$, $K = \Omega(Y, *)$. Для $\varphi \in Y'$ обозначим $\widehat{\varphi} = P'\varphi$; таким образом, $\widehat{\varphi} \in X'$, $\widehat{\varphi}\big|_Y = \varphi$ и $\widehat{\varphi}\big|_{(I-P)(X)} = 0$. Выберем $\varphi \in K$ и положим

$$\circ : X^2 \to X, \quad x \circ y = \widehat{\varphi}(x)y + \widehat{\varphi}(y)x - \widehat{\varphi}(x)\widehat{\varphi}(y)e + (Px - \widehat{\varphi}(x)e) * (Py - \widehat{\varphi}(y)e).$$

Как нетрудно проверить, $\circ \in \mathscr{M}(X)$, e служит единицей в $(X, \circ)$ и $\widehat{\varkappa} \in \Omega(X, \circ)$ для всякого $\varkappa \in \Omega(Y, *)$. Пусть теперь $\varphi \in \Omega(X, \circ)$ и $\varkappa = \varphi\big|_Y$. Так как $x \circ x = 0$ для каждого $x \in (I - P)(X)$, имеем $\widehat{\varphi}\big|_{(I-P)(X)} = 0$ и поэтому $\varphi = \widehat{\varkappa}$. Таким образом, отображение $\varkappa \mapsto \widehat{\varkappa}$ является непрерывным инъективным отображением (а следовательно, гомеоморфизмом) из K в $\Omega(X, \circ)$. Отсюда $\mathscr{K}(Y) \subset \mathscr{K}(X)$. □

Предложение 2. *Пусть X — банахово пространство, а $P_1, \ldots, P_n$ — линейные непрерывные проекции X, обладающие свойством $P_j P_k = 0$ при $j \neq k$. Тогда $\mathscr{K}(X)$ содержит сумму классов $\mathscr{K}(P_j(X))$.*

Доказательство. Пусть $*_j \in \mathscr{M}(P_j(X))$, $K_j = \Omega(P_j(X), *_j)$ и e_j — единица $(P_j(X), *_j)$. Согласно предложению 1, так как сумма подпространств $P_j(X)$ дополняема, можно без потери общности предположить, что $P_1 + \cdots + P_n = I$. Положим

$$* : X^2 \to X, \quad x * y = \sum_{j=1}^{n} P_j x *_j P_j y.$$

Нетрудно убедиться, что $* \in \mathscr{M}(X)$, $e = e_1 + \cdots + e_n$ является единицей $(X, *)$ и функционал $\varphi \in X'$ принадлежит $\Omega(X, *)$ тогда и только тогда, когда все ограничения φ на $P_j(X)$ равны нулю, кроме одного, принадлежащего K_j. Это наблюдение показывает, что $\Omega(X, *)$ гомеоморфно дизъюнктному открыто-замкнутому объединению пространств K_n. Таким образом, $\mathscr{K}(X)$ содержит сумму $\mathscr{K}(P_j(X))$. □

Предложение 3. *Пусть X — банахово пространство, а P_k, $k \in \mathbb{N}$ — линейные проекции на X, причем $P_j P_k = 0$ при $j \neq k$ и сумма подпространств $P_k(X)$ неплотна в X. Тогда $\mathscr{K}(X)$ содержит сумму классов $\mathscr{K}(P_k(X))$.*

Доказательство. Пусть $*_j \in \mathscr{M}(P_j(X))$, $K_j = \Omega(P_j(X), *_j)$ и e_j — единицы в $(P_j(X), *_j)$. Поскольку сумма $P_n(X)$ не плотна в X, существует такой функционал $\varphi \in X' \setminus \{0\}$, что $\varphi\big|_{P_n(X)} = 0$ при всех $n \in \mathbb{N}$. Выберем вектор $e \in X$, для которого $\varphi(e) = 1$. Так как

$$b_n = \sup\{\|x *_n y\| : x, y \in P_n(X),\ \|x\| \leqslant 1,\ \|y\| \leqslant 1\} < \infty,$$

существуют такие числа $c_n \in (0, \infty)$, что $\sum c_n b_n \|P_n\|^2 < +\infty$. Очевидно, отображение

$$* : X^2 \to X, \quad x * y = \varphi(x)y + \varphi(y)x - \varphi(x)\varphi(y)e + \sum c_n P_n x *_n P_n y$$

корректно определено. Непосредственная проверка показывает, что $* \in \mathscr{M}(X)$ и e является единицей в $(X, *)$. Для $n \in \mathbb{N}$ и $f \in K_n$ пусть $\widehat{f} \in X'$ — такой функционал, что $\widehat{f}\big|_{P_n(X)} = f$ и $\widehat{f}\big|_{(I-P_n)(X)} = 0$. Несложно проверить, что

$$\Omega(X, *) = \{\varphi\} \cup \bigcup_{n \in \mathbb{N}} \{\varphi + c_n \widehat{f} : f \in K_n\}.$$

Очевидно, спектр $\Omega(X, *)$ гомеоморфен александровской компактификации дизъюнктного открыто-замкнутого объединения пространств K_n. Таким образом, $\mathscr{K}(X)$ содержит сумму $\mathscr{K}(P_j(X))$. □

Предложение 4. *Пусть $X_1, X_2, \ldots, X_n$ — банаховы пространства. Тогда $\mathscr{K}(X) \supseteq \prod \mathscr{K}(X_j)$, где $X = X_1 \widehat{\otimes} \ldots \widehat{\otimes} X_n$.*

Доказательство см. в [6], § 2.3.

Предложение 5. *Пусть X — банахово пространство, изоморфное $X \times \mathbb{C}$. Тогда класс $\mathscr{K}(X)$ замкнут относительно конечных склеиваний.*

Доказательство. Пусть $* \in \mathscr{M}(X)$, $K = \Omega(X, *)$, e — единица в $(X, *)$ и $\varkappa_1, \varkappa_2 \in K$. Достаточно показать, что результат K_1 склеивания точек $\varkappa_1$ и $\varkappa_2$ является элементом $\mathscr{K}(X)$. Пусть $Y = \{x \in X : \varkappa_1(x) = \varkappa_2(x)\}$. Множество Y является подалгеброй в $(X, *)$ и замкнутой гиперплоскостью в банаховом пространстве X. Так как X изоморфно $X \times \mathbb{C}$, пространство Y изоморфно X. Остается убедиться, что спектр $\Omega(Y, *)$ гомеоморфен K_1. Очевидно, отображение ξ, сопоставляющее классу эквивалентности из K_1 сужение некоторого представителя этого класса на Y, непрерывно и взаимно однозначно отображает K_1 в $\Omega(Y, *)$. Остается проверить сюръективность ξ, т.е. показать, что каждый характер $(Y, *)$ является ограничением на Y некоторого характера $(X, *)$. Пусть $\varkappa \in \Omega(Y, *)$. Заметим, что элемент $x \in Y$ обратим в X тогда и только тогда, когда он обратим в Y, так как из $xx^{-1} = e$ и $\varkappa_1(x) = \varkappa_2(x)$ следует, что $\varkappa_1(x^{-1}) = \varkappa_2(x^{-1})$. Таким образом, идеал I, порожденный множеством $\ker \varkappa$ в алгебре X, является собственным в X, поскольку $\ker \varkappa$ не содержит обратимых элементов. Далее, в X существует максимальный идеал J, содержащий I [6], который определяет единственным образом некоторый характер $\bar{\varkappa} \in K$. Очевидно, $\bar{\varkappa}$ продолжает $\varkappa$. □

4. Основные результаты

Теорема 1. 1) *Для всякого бесконечномерного банахова пространства X верно соотношение $\mathscr{S}_1 \subseteq \mathscr{K}(X)$.*
2) *Для всякого сепарабельного банахова пространства X верно соотношение $\mathscr{K}(X) \subseteq \mathscr{S}_{\mathrm{me}}$.*
3) *Для всякого банахова пространства X, содержащего дополняемое подпространство с бесконечным безусловным базисом Шаудера, верно соотношение $\mathscr{S}_\omega \subseteq \mathscr{K}(X)$.*

Из теоремы 1 и предложений 2, 3 и 5 вытекает следующее утверждение.

Следствие 1. *Пусть X — сепарабельное банахово пространство, изоморфное X^2 и $X \times \mathbb{C}$. Тогда $\mathscr{S}_\omega \subset \mathscr{K}(X) \subset \mathscr{S}_{\mathrm{me}}$ и класс $\mathscr{K}(X)$ замкнут относительно конечных и бесконечных сумм и относительно конечных склеиваний.*

Заметим, что все банаховы пространства, естественно возникающие в анализе, удовлетворяют условиям следствия 1.

Теорема 2. *Пусть X — наследственно неразложимое сепарабельное банахово пространство. Тогда $\mathscr{K}(X^n) = \mathscr{S}_n$ при всех $n \in \mathbb{N}$.*

Теорема 2 показывает, что отображение $X \mapsto \mathscr{K}(X)$ принимает бесконечно много различных значений.

Теорема 3. $\mathscr{K}(C[0,1]) = \mathscr{K}_{\mathrm{me}}$.

Следующее утверждение показывает, что классы $\mathscr{K}(l_p)$, $\mathscr{K}(c_0)$ и $\mathscr{K}(L_p[0,1])$ содержат некоторые несчетные компактные пространства.

Предложение 6. *Пусть $X \in \{c_0\} \cup \{l_p : 1 \leqslant p < \infty\} \cup \{L_p[0,1] : 1 \leqslant p < \infty\}$. Тогда $\mathbb{T}^n \in \mathscr{K}(X)$ для всех $n \in \mathbb{N}$.*

Заметим, что, внеся небольшие изменения в доказательство предложения 6 (рассматривая полиномы Чебышева вместо функций e^{inx} и изменив некоторые детали), можно заменить в предложении 6 пространство $\mathbb{T}^n$ на $\mathbb{T}^n \times [-1,1]^m$ для произвольных $n, m \in \mathbb{Z}_+$, $m + n > 0$.

Предложение 7. *Класс $\mathscr{K}(l_2)$ содержит все конечномерные метризуемые компактные пространства, а класс $\mathscr{K}(l_1)$ содержит $\mathscr{S}_{\mathrm{mag}}$.*

4.1. Доказательство теоремы 1. Так как пространство, на котором существует разделяющее точки счетное множество непрерывных функций, метризуемо [9], для всякого сепарабельного банахова пространства $\mathscr{K}(X) \subset \mathscr{S}_{me}$.

Пусть X — бесконечномерное банахово пространство. Тогда существует последовательность линейных непрерывных проекций P_n на X, имеющих одномерные образы и удовлетворяющих условиям предложения 3. Из предложений 2 и 3 следует, что $\mathscr{K}(X)$ содержит конечные отделимые компактные пространства и александровскую компактификацию счетного дискретного пространства. Таким образом, $\mathscr{S}_1 \subseteq \mathscr{K}(X)$. Отметим, что другое доказательство включения $\mathscr{S}_1 \subseteq \mathscr{K}(X)$ можно получить, анализируя доказательство основного результата [2].

Пусть $\mathscr{K} = \bigcap\{\mathscr{K}(X) : X \in \mathscr{B}_{\mathrm{ub}}\}$, где $\mathscr{B}_{\mathrm{ub}}$ обозначает класс банаховых пространств со счетным безусловным базисом Шаудера. Так как для данного $X \in \mathscr{B}_{\mathrm{ub}}$ существует последовательность линейных непрерывных проекций P_n на X, образы которых сами принадлежат классу $\mathscr{B}_{\mathrm{ub}}$, из предложений 2 и 3 следует, что класс $\mathscr{K}$ замкнут относительно конечных и счетных сумм. Так как $\mathscr{S}_1 \subseteq \mathscr{K}$ и $\mathscr{S}_\omega$ является минимальным классом хаусдорфовых компактных топологических пространств, содержащим $\mathscr{S}_1$ и замкнутым относительно конечных и счетных сумм [9], получаем $\mathscr{S}_\omega \subseteq \mathscr{K}$. Теорема 1 следует теперь из предложения 1.

4.2. Доказательство теоремы 2. Пусть X и Y — банаховы пространства. Напомним, что оператор $T \in L(X,Y)$ называется *строго сингулярным*, если для каждого замкнутого линейного подпространства Z пространства X его образ $T(Z)$ либо конечномерен, либо незамкнут; оператор T называется *фредгольмовым*, если пространства $\ker T$ и $Y/T(X)$ конечномерны.

В [10,16] содержится следующий результат.

Лемма 1. *Пусть X — наследственно неразложимое банахово пространство и $T \in L(X,X)$. Тогда существует единственное число $\lambda(T) \in \mathbb{C}$ такое, что оператор $T - \lambda(T)I$ строго сингулярен.*

Из того факта, что строго сингулярные операторы образуют идеал в алгебре операторов [15], следует, что отображение $T \mapsto \lambda(T)$ из леммы 1 является непрерывным линейным функционалом на банаховом пространстве $L(X,X)$. Следующая лемма для случая $n = 1$ также доказана в [10].

Лемма 2. *Пусть X — наследственно неразложимое банахово пространство, $n \in \mathbb{N}$, $T \in L(X^n, X^n)$ и $\sigma(T)$ — спектр оператора T. Тогда существует множество $M = M(T) \subset \mathbb{C}$, состоящее не более чем из n точек, такое, что все точки $\lambda \in \sigma(T) \setminus M$ являются изолированными точками $\sigma(T)$ и собственными значениями T конечной кратности.*

Доказательство. В доказательстве мы отождествляем $\mathbb{C}^n \otimes X$ с X^n. Для $1 \leqslant i \leqslant n$ и $1 \leqslant j \leqslant n$ пусть $T_{ij} \in L(X,X)$ — оператор, определенный формулой $T_{ij}x = (T(e_j \otimes x))_i$, где через e_i обозначены векторы стандартного базиса $\mathbb{C}^n$. Пусть $\lambda_{ij} = \lambda(T_{ij})$, где λ обозначает функционал из леммы 1, $\Lambda_0 \in L(\mathbb{C}^n, \mathbb{C}^n)$ — оператор с матрицей λ_{ij}, а M — спектр Λ_0. Очевидно, M состоит не более чем из n точек. Пусть $\Lambda = \Lambda_0 \otimes I \in L(X^n, X^n)$. Так как операторы $T_{ij} - \lambda_{ij}I$ строго сингулярны, $A = T - \Lambda$ также строго сингулярен. Рассмотрим отображение $\Phi : \mathbb{C} \setminus M \to L(X^n, X^n)$, $\Phi(z) = T - zI = \Lambda - zI + A$. Так как спектр Λ совпадает с M, оператор $\Lambda - zI$ обратим и потому фредгольмов. В [15] показано, что всякий строго сингулярный оператор является оператором Рисса и потому сумма фредгольмова и строго сингулярного оператора является фредгольмовым оператором. Таким образом, голоморфная функция Φ, определенная на области в $\mathbb{C}$, принимает значения во множестве фредгольмовых операторов, и оператор $\Phi(z)$ обратим при некоторых z (например, если $|z| > \|T\|$). Из основного результата [11] следует, что $\Phi(z)$ может быть необратимым только в некоторых изолированных точках z (в этих точках пространство $\ker \Phi(z)$ конечномерно, так как оператор $\Phi(z)$ является фредгольмовым). По определению $\Phi(z)$ все точки $\lambda \in \sigma(T) \setminus M$ являются изолированными точками $\sigma(T)$ и собственными значениями T конечной кратности. □

Теперь мы может доказать теорему 2. Из теоремы 1 и предложений 1 и 2 следует, что $\mathscr{S}_n \subset \mathscr{K}(X^n)$. Пусть $* \in \mathscr{M}(X^n)$. Остается показать, что $K = \Omega(X^n, *)$ имеет не более n неизолированных точек. Предположим противное. Тогда существуют попарно различные неизолированные в K точки $\varkappa_1, \ldots, \varkappa_{n+1} \in K$. Для вектора $x \in X^n$ обозначим $T_x \in L(X^n, X^n)$, $T_x y = x * y$. Так как $(X^n, *)$ является коммутативной банаховой алгеброй, спектр $\sigma_x = \sigma(T_x)$ совпадает со множеством $\{\varkappa(x) : \varkappa \in K\}$ [6]. Согласно лемме 2 это множество имеет не более n неизолированных точек. Очевидно, точка $\varkappa_j(x)$ неизолирована в σ_x тогда и только тогда, когда функция $\varkappa \mapsto \varkappa(x)$ постоянна в некоторой окрестности каждой неизолированной точки $\varkappa$ в K, для которой $\varkappa(x) = \varkappa_j(x)$. Поскольку число точек $\varkappa_j$ равно $n+1$, а множество σ_x имеет не более n неизолированных точек, получаем, что либо существуют числа i, j, для которых $1 \leqslant i < j \leqslant n+1$ и $\varkappa_i(x) = \varkappa_j(x)$, либо существуют число $1 \leqslant j \leqslant n+1$ и окрестность O точки $\varkappa_j$ в K такие, что функция $\varkappa \mapsto \varkappa(x)$ постоянна на O. Выберем метрику d, задающую топологию K. Так как x — произвольная точка X^n, получаем, что

$$X^n = \bigcup_{1 \leqslant i < j \leqslant n+1} L_{ij} \cup \bigcup_{\substack{1 \leqslant k \leqslant n+1 \\ m \in \mathbb{N}}} M_{km}, \tag{1}$$

где

$$L_{ij} = \{x \in X^n : \varkappa_i(x) = \varkappa_j(x)\}, \quad M_{km} = \{x \in X^n : \varkappa(x) = \varkappa_k(x) \text{ при } d(\varkappa, \varkappa_k) \leqslant m^{-1}\}.$$

Так как L_{ij} и M_{km} являются собственными замкнутыми линейными подпространствами банахова пространства X^n, формула (1) противоречит теореме Бэра [1]. Таким образом, K имеет не более n неизолированных точек.

4.3. Доказательство теоремы 3. Так как банахово пространство c_0 обладает безусловным базисом Шаудера и изоморфно дополняемому подпространству $C[0,1]$, из предложения 2 и теоремы 1 следует, что $\mathscr{S}_\omega \subseteq \mathscr{K}(C[0,1])$. Пусть K — несчетное компактное метрическое пространство. По теореме Милютина [13, 14] банаховы пространства $C[0,1]$ и $C(K)$ изоморфны. Поскольку спектр $C(K)$ с поточечным умножением гомеоморфен K [6], получаем, что $K \in \mathscr{K}(C[0,1])$. Поэтому $\mathscr{K}(C[0,1])$ содержит все несчетные метрические компактные пространства. Таким образом, $\mathscr{K}(C[0,1]) = \mathscr{S}_{\mathrm{me}}$.

4.4. Доказательство предложения 6. Для $k \in \mathbb{Z}$ и $q \in (1,+\infty)$ обозначим $\rho(k) = \max\{1,|k|\}$, $\beta_q(k) = \sum\limits_{j\in\mathbb{Z}} \rho(j)^{-q}\rho(k-j)^{-q}$. Конечность $\beta_q(k)$ очевидна. Следующая техническая лемма представляет собой элементарное упражнение: достаточно рассмотреть отдельно монотонные части суммы в определении $\beta_q(k)$ и оценить каждую с помощью соответствующего интеграла.

Лемма 3. *Для каждого $q \in (1,+\infty)$ существует такое число $c = c(q) > 0$, что неравенство $\beta_q(k) \leqslant c\rho(k)^{-q}$ выполняется при всех $k \in \mathbb{Z}$.*

Пусть $n \in \mathbb{N}$ и пространство $E = C^\infty(\mathbb{T}^n)$ наделено нормой $\|\cdot\|$, для которой существует такая константа $c > 0$, что

$$\|fg\| \leqslant c\|f\|\|g\| \quad \forall f,g \in E, \tag{2}$$

$$\sup_{x\in\mathbb{T}^n} |f(x)| \leqslant c\|f\| \quad \forall f \in E. \tag{3}$$

Из условий (3) следует, что тождественное вложение $J_0 : E \to C(\mathbb{T}^n)$ непрерывно и потому продолжается единственным образом до отображения $J : X \to C(\mathbb{T}^n)$, определенного на пополнении X пространства E. Более того, согласно (2) X является банаховой алгеброй с единицей относительно (продолженного) поточечного умножения, а J является морфизмом банаховых алгебр X и $C(\mathbb{T}^n)$. Для $t \in \mathbb{T}^n$ положим $\varkappa_t \in X'$, $\varkappa_t(f) = Jf(t)$. Очевидно, отображение $t \mapsto \varkappa_t$ инъективно отображает $\mathbb{T}^n$ в $\Omega(X)$. Пусть теперь K — компактное подмножество $\mathbb{T}^n$, $I = \{f \in X : \varkappa_t(f) = 0\ \forall t \in K\}$ и $H = X/I$ (очевидно, I — замкнутый идеал в X).

Лемма 4. *Спектр $\Omega = \Omega(H)$ гомеоморфен K.*

Доказательство. Пусть $\varphi : K \to \Omega$, $\varphi(t)(f+I) = \varkappa_t(f)$. Очевидно, отображение φ корректно определено и взаимно однозначно. Остается показать, что оно сюръективно. Предположим, что существует характер $\varkappa \in \Omega \setminus \varphi(K)$. Тогда для любой точки $t \in K$ существует вектор $f_t \in E$ такой, что $\varkappa(f_t + I) = 0$ и $f_t(t) = 1$ (иначе $\varkappa$ равен нулю на множестве $E/(E \cap I)$, плотном в H). Пусть $U_t = \{s \in \mathbb{T}^n : f_t(s) \neq 0\}$. Множества $\{U_t : t \in K\}$ образуют открытое покрытие компактного пространства K. Выберем конечное подпокрытие $\{U_{t_1},\dots,U_{t_m}\}$ и рассмотрим $g = \sum f_{t_j}\overline{f_{t_j}} \in E$. Тогда $g(t) \neq 0$ при всех $t \in K$ и по теореме продолжения Уитни [17] существует $h \in E$ со свойством $h(t) = 1/g(t)$ при $t \in K$. Тогда $\varkappa(g+I) = 0$ и $(h+I)(g+I)$ — единица H. Таким образом, ненулевой характер $\varkappa$ обращается в нуль на обратимом элементе $g+I$, что невозможно. □

Пусть $1 \leqslant p \leqslant \infty$, $F_k : \mathbb{T} \to \mathbb{C}$, $F_k(t) = e^{ikt}$ $(k \in \mathbb{Z})$. Для $\mathbf{k} \in \mathbb{Z}^n$ пусть функция $F_{\mathbf{k}} : \mathbb{T}^n \to \mathbb{C}$ определяется формулой

$$F_{\mathbf{k}}(x) = F_{k_1}(x_1)\dots F_{k_n}(x_n).$$

Известно [4], что каждая функция $f \in E$ допускает единственное представление в виде равномерно сходящегося ряда вида

$$f(x) = \sum_{\mathbf{k}\in\mathbb{Z}^n} f_{\mathbf{k}}F_{\mathbf{k}}(x), \tag{4}$$

и $|f_{\mathbf{k}}| = O((|k_1| + \dots + |k_n|)^{-\alpha})$ для любого $\alpha > 0$. Рассмотрим норму

$$\|f\| = \begin{cases} \sum |f_{\mathbf{k}}|, & \text{если } p = 1, \\ \left(\sum \rho(\mathbf{k})^p |f_{\mathbf{k}}|^p\right)^{1/p}, & \text{если } 1 < p < \infty, \\ \sup \rho(\mathbf{k})^2 |f_{\mathbf{k}}|, & \text{если } p = \infty, \end{cases} \tag{5}$$

где $\rho(\mathbf{k}) = \rho(k_1) \dots \rho(k_n)$. Очевидно, это выражение корректно задает норму на E, удовлетворяет условию (3), а пополнение X пространства E по этой норме изоморфно l_p при $p < \infty$ и c_0 при $p = \infty$. Остается проверить выполнение неравенства (2). В самом деле, если (2) выполнено, из леммы 4 с $K = \mathbb{T}^n$ следует, что X с поточечным умножением является коммутативной банаховой алгеброй со спектром, гомеоморфным $\mathbb{T}^n$.

*С*лучай 1: $p = 1$. Для любых $f, g \in E$ имеем

$$\|fg\| = \sum_{\mathbf{k}} \left| \sum_{\mathbf{m}+\mathbf{j}=\mathbf{k}} f_{\mathbf{m}} g_{\mathbf{j}} \right| \leqslant \sum_{\mathbf{m},\mathbf{j}} |f_{\mathbf{m}} g_{\mathbf{j}}| = \|f\| \|g\|.$$

*С*лучай 2: $p = \infty$. В этом случае

$$\|fg\| = \sup_{\mathbf{k}} \rho(\mathbf{k})^2 \left| \sum_{\mathbf{m}+\mathbf{j}=\mathbf{k}} f_{\mathbf{m}} g_{\mathbf{j}} \right| \leqslant \|f\| \|g\| \sup_{\mathbf{k}} \sum_{\mathbf{m}+\mathbf{j}=\mathbf{k}} \frac{\rho(\mathbf{k})^2}{\rho(\mathbf{m})^2 \rho(\mathbf{j})^2} \leqslant \sup_{k \in \mathbb{Z}} \rho(k)^{2n} \beta_2(k)^n \|f\| \|g\|.$$

С помощью леммы 3 из этого неравенства следует (2).

*С*лучай 3: $1 < p < \infty$. Используя неравенство Гельдера, получаем

$$\|fg\|^p = \sum_{\mathbf{k} \in \mathbb{Z}^n} \rho(\mathbf{k})^p \left| \sum_{\mathbf{j}+\mathbf{m}=\mathbf{k}} f_{\mathbf{j}} g_{\mathbf{m}} \right|^p \leqslant \sum_{\mathbf{k} \in \mathbb{Z}^n} \rho(\mathbf{k})^p A_{\mathbf{k}} B_{\mathbf{k}}^p,$$

где

$$A_{\mathbf{k}} = \left(\sum_{\mathbf{m}+\mathbf{j}=\mathbf{k}} \rho(\mathbf{m})^p |f_{\mathbf{m}}|^p \rho(\mathbf{j})^p |g_{\mathbf{j}}|^p \right), \quad B_{\mathbf{k}} = \left(\sum_{\mathbf{m}+\mathbf{j}=\mathbf{k}} \rho(\mathbf{m})^{-q} \rho(\mathbf{j})^{-q} \right)^{1/q}$$

и $p^{-1} + q^{-1} = 1$. Очевидно, $\sum A_{\mathbf{k}} = \|f\|^p \|g\|^p$ и $\rho(\mathbf{k}) B_{\mathbf{k}} \leqslant C^{n/q}$, где $C = \sup\limits_{k \in \mathbb{Z}} \rho(k)^q \beta_q(k)$. Согласно лемме 3 имеем $C < \infty$. Поэтому $\|fg\| \leqslant C^{n/q} \|f\| \|g\|$, и неравенство 2 доказано.

4.5. Доказательство предложения 7. Пусть K — метризуемая абелева компактная топологическая группа. Тогда группа ее характеров K^+ (см. [7]) счетна и дискретна. Дискретность K^+ означает, что банахово пространство $L_1(K^+, m)$ (m — мера Хаара) изоморфно l_1. Известно [6, 7], что K гомеоморфно спектру $\Omega(L_1(K^+, m), *)$, где символ $*$ обозначает свертку, и потому $K \in \mathscr{K}(l_1)$. Таким образом, $\mathscr{S}_{\text{mag}} \subset \mathscr{K}(l_1)$.

Пусть $n \in \mathbb{N}$, K — компактное подмножество $\mathbb{T}^n$, пространство $E = C^\infty(\mathbb{T}^n)$ наделено нормой (5) при $p = 2$. Согласно лемме 4 существует коммутативная банахова алгебра H, изоморфная l_2 как банахово пространство и имеющая спектром K. Остается заметить, что всякое метризуемое компактное пространство топологической размерности m гомеоморфно вкладывается в $\mathbb{T}^n$ при $n = 2m + 1$ [5]. Таким образом, $\mathscr{K}(l_2)$ содержит все конечномерные метризуемые компактные пространства.

Заметим, что вместо того чтобы рассматривать пространство E с нормой (5), можно было рассмотреть норму, индуцированную (гильбертовым) пространством Соболева функций на $[-1, 1]^n$ или $\mathbb{T}^n$ гладкости, достаточной для применения соответствующей теоремы вложения [3].

5. Открытые вопросы

Как уже говорилось, основной целью статьи является привлечение внимания к предлагаемой классификации банаховых пространств. Конечно, здесь предложено больше вопросов, чем ответов. Мы перечислим лишь несколько нерешенных проблем, которые кажутся нам интересными и естественными.

1. Описание классов $\mathscr{K}(X)$ для частных банаховых пространств, естественно возникающих в анализе. Например, каков класс $\mathscr{K}(X)$ при $X = c_0$ или $X = l_p$, $1 \leqslant p \leqslant \infty$?
2. Содержит ли $\mathscr{K}(X)$ при несепарабельном банаховом пространстве X неметризуемые компактные пространства?
3. Существует ли банахово пространство X со счетным бесконечным безусловным базисом, для которого $\mathscr{K}(X) = \mathscr{S}_\omega$?

Благодарности. Авторы благодарны профессорам О. Г. Смолянову и А. Я. Хелемскому за интерес к работе и замечания. С. Ш. благодарит фонд Александра фон Гумбольдта за поддержку.

СПИСОК ЛИТЕРАТУРЫ

1. *Колмогоров А. Н., Фомин С. В.* Элементы теории функций и функционального анализа. — М.: Наука, 1981.
2. *Кузнецова Ю. Н.* Об умножении в пространствах Фреше// Вестн. МГУ. Сер. мат., мех. — 2001. — *56*. — С. 58–61.
3. *Ладыженская О. А., Уральцева Н. Н.* Линейные и квазилинейные уравнения эллиптического типа. — М.: Наука, 1973.
4. *Пич А.* Ядерные локально выпуклые пространства. — М.: Мир, 1967.
5. *Понтрягин Л. С.* Основы комбинаторной топологии. — М.: Наука, 1986.
6. *Хелемский А. Я.* Банаховы и полинормированные алгебры. Общая теория, представления, гомологии. — М.: Наука, 1989
7. *Хьюитт Э., Росс К.* Абстрактный гармонический анализ. — М.: Наука, 1975.
8. *Шефер Х.* Топологические векторные пространства. — М.: Мир, 1971.
9. *Энгелькинг Р.* Общая топология. — М.: Мир, 1986.
10. *Gowers W. T., Mourey B.* The unconditional basic sequence problem// J. Amer. Math. Soc. — 1993. — *6*. — С. 851–874.
11. *Gramsch B.* Inversion von Fredholmfunktionen bei stetiger und holomorpher Abhängingkeit von Parametern// Math. Ann. — 1975. — *214*. — С. 95–147.
12. *Lindenstrauss J., Tsafriri L.* Classical Banach spaces. — Berlin, Heidelberg: Springer-Verlag, 1996.
13. *Milyutin A.* Isomorphism of two spaces of continuous functions over compact sets of cardinality of the continuum// Funct. Anal. Appl. — 1966. — *2*. — С. 150–156.
14. *Pelczinski A.* Linear extensions, linear averaging and their applications to linear topological classification of spaces of continuous functions// Rozprawy Mat. — 1968. — *58*.
15. *Pietsch A.* Operator ideals. — Amsterdam: North-Holland, 1980.
16. *Räbiger F., Richer W. J.* C_0-Groups and C_0-semigroups of linear operators on hereditarily indecomposable Banach spaces// Arch. Math. — 1996. — *66*. — С. 60–70.
17. *Stein E.* Singular integrals and differentiability properties of functions. — Princeton: Princeton Univ. Press, 1970.

С. А. Шкарин
Московский государственный университет
E-mail: shkarin@math.uni-wuppertal.de

Ю. Н. Кузнецова
Московский государственный университет
E-mail: juglans@rambler.ru

Современная математика и ее приложения. Том 14 (2004). С. 108–120

УДК 512.62

КРИТЕРИЙ ПОЛНОТЫ ПЕРИОДА МНОГОЧЛЕНА ГАЛУА НАД СОБСТВЕННЫМ КОЛЬЦОМ ГАЛУА НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

© 2004 г. **В. Н. ЦЫПЫШЕВ**

Аннотация. В настоящей работе предлагается критерий полноты периода многочлена Галуа над кольцом Галуа, выраженный в терминах коэффициентов этого многочлена. При этом рассматривается случай кольца Галуа нечетной характеристики, отличного от поля и кольца вычетов. Такое кольцо Галуа мы далее называем *собственным*. Проведенные вычислительные эксперименты показывают, что предложенный критерий является полезным и удобным при использовании на практике.

СОДЕРЖАНИЕ

1. Введение

В последнее время линейные рекуррентные последовательности стали предметом активного изучения ввиду важности их приложений в криптографии и теории кодирования, где они используются как источник псевдослучайных значений. В каждой из этих областей весьма полезно иметь практический способ построения линейных рекуррент максимально возможного периода. Обычно это делается путем построения многочлена максимального периода, после чего линейная рекуррента генерируется путем применения построенного многочлена.

История предмета отражена в [12]. Отметим, что важнейший шаг в развитии теории построения многочленов максимального периода над конечными коммутативными кольцами главных иделов был сделан А. А. Нечаевым. Кроме того, он же предложил способ использования его собственных общих результатов в частном случае примарных колец вычетов четной характеристики и колец Галуа четной характеристики.

В случае примарных колец вычетов нечетной характеристики практический способ построения многочленов максимального периода был предложен А. С. Кузьминым.

В дальнейшем будет удобно кольцо Галуа, не являющееся ни конечным полем, ни примарным кольцом вычетов, называть *собственным*.

В настоящей работе предложен способ построения многочленов максимального периода над кольцом Галуа в ранее не рассматривавшемся случае собственных колец Галуа нечетной характеристики.

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа порядка q^n, $q = p^r$, и характеристики p^n [13, 14]. Многочлен $F(x)$ над кольцом R называется *реверсивным*, если его свободный член является обратимым элементом кольца R.

Пусть $F(x) \in R[x]$ — унитарный реверсивный многочлен над кольцом R. Всюду далее $\mathrm{T}(F)$ обозначает период многочлена $F(x)$ — наименьшее $t \in \mathbb{N}_0$, обладающее свойством $F(x) \mid x^t - e$.

ISSN 1512–1712

Напомним [11, 12], что имеют место соотношения

$$\mathrm{T}(\bar{F}(x)) \mid \mathrm{T}(F(x)) \mid \mathrm{T}(\bar{F}(x)) \cdot p^{n-1}.$$

Многочлен $F(x)$ называется *отмеченным*, если $\mathrm{T}(F) = \mathrm{T}(\bar{F})$, и *многочленом полного периода*, если $\mathrm{T}(F) = \mathrm{T}(\bar{F}) \cdot p^{n-1}$. Если при этом $\mathrm{T}(\bar{F}) = q^m - 1$, то $F(x)$ называется *многочленом максимального периода* (МП-многочленом).

Унитарный и реверсивный одновременно многочлен над кольцом R называется *регулярным*. Многочлен $F(x)$ называется *сепарабельным*, если $\gcd(F(x), F'(x)) = e$, где $F'(x)$ обозначает производную. Отмеченный многочлен $G(x)$ называется *соответствующим* многочлену $F(x)$, если $\bar{G}(x) = \bar{F}(x)$. Известно [11], что для каждого регулярного сепарабельного многочлена $F(x)$ над кольцом Галуа R существует единственный сравнимый с ним по модулю pR отмеченный многочлен $F_*(x)$. Многочлен $F_*(x)$ будем называть *отмеченным многочленом, соответствующим многочлену* $F(x)$. Многочлен $F(x)$ называется многочленом *Галуа*, если он унитарный, а многочлен $\bar{F}(x)$ — образ многочлена $F(x)$ при каноническом эпиморфизме $R[x] \to R[x]/pR[x]$ — является неприводимым над полем $\bar{R} = R/pR$.

Ниже предлагается алгоритм, позволяющий по заданному многочлену Галуа за фиксированное число шагов построить соответствующий ему отмеченный многочлен. Кроме того, рассматривается вопрос о критерии полноты периода многочлена Галуа над кольцом Галуа.

Ранее такой критерий был найден А. А. Нечаевым, который получил следующие результаты.

Теорема 1.1 (см. [11]). *Многочлен Галуа $F(x)$ степени m над кольцом Галуа $R = GR(q^n, p^n)$ является многочленом полного периода тогда и только тогда, когда выполнены следующие эквивалентные условия.*

(a) *Если $F_*(x)$ — отмеченный многочлен, соответствующий $F(x)$, то*

$$F(x) = F_*(x) + pV(x),$$

где $\bar{V}(x) \neq \bar{0}$; при $p = 2 < n$, кроме того, $\bar{V}(x) \not\equiv x\bar{F}'(x) \pmod{\bar{F}(x)}$.

(b) *Если $\tau = \mathrm{T}(\bar{F})$, то*

$$x^\tau \equiv e + p\Phi(x) \pmod{F(x)}, \quad \deg\Phi(x) < m, \quad \bar{\Phi}(x) \neq \bar{0};$$

в случае $p = 2 < n$, кроме того,

$$\bar{\Phi}(x) \neq \bar{e}.$$

Этот критерий является неудобным с точки зрения практического его применения, поскольку требует либо нахождения соответствующего $F(x)$ отмеченного многочлена, либо нахождения вычета $\operatorname{Res} x^\tau \bmod F(x)$

В связи с этим А. А. Нечаевым был предложен следующий критерий максимальности периода многочлена над кольцом $\mathbb{Z}_{2^n}$.

Теорема 1.2 (см. [11, 12]). *Если $R = \mathbb{Z}_{2^n}$, многочлен $F(x) = \sum\limits_{j\geqslant 0} f_j x^j \in R[x]$ представлен в виде*

$$F(x) = F^{(0)}(x^2) + xF^{(1)}(x^2),$$

где $F^{(t)}(x) = \sum\limits_{j\geqslant 0} f_{t+2j}x^j$, $t = \overline{0,1}$, а многочлен $F_1(x)$ определен равенством

$$F_1(x) = (-1)^m \left(F^{(0)}(x)^2 - xF^{(1)}(x)^2\right),$$

то имеет место соотношение

$$F(x) - F_1(x) = 2\Delta(x).$$

При этом $\mathrm{T}(F) = (2^m - 1)2^{n-1}$ в том и только в том случае, когда одновременно выполнены следующие условия:

(a) $\mathrm{T}(\bar{F}) = 2^m - 1$;

(b) $\bar{\Delta}(x) \neq 0$ *и при* $n > 2$ *имеем* $\bar{\Delta}(x) \not\equiv x\bar{F}'(x) \pmod{\bar{F}(x)}$.

При выполнении условия (a) *произвольный многочлен вида* $H(x) = F_1(x) + 2D(x)$, *где* $\deg D(x) < m$, *является МП-многочленом тогда и только тогда, когда многочлен* $D(x)$ *удовлетворяет условию* (b) (*где* Δ *заменяется на* D).

В развитие предыдущей теоремы А. С. Кузьминым был предложен критерий полноты периода многочлена Галуа над примарным кольцом вычетов по модулю p^n, $p \geqslant 3$, зависящий только от коэффициентов этого многочлена.

Теорема 1.3 (см. [5]). *Пусть* $F(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ — *реверсивный* (*т.е. с обратимым свободным членом*) *многочлен над кольцом* $\mathbb{Z}_{p^n}$, $p \geqslant 3$, *и* $\mathrm{T}(\bar{F}) = p^m - 1$. $F(x)$ *является МП-многочленом, если и только если выполнено условие*

$$\sum_{(j_0,\ldots,j_m)\in A} \frac{p!}{j_0!\cdots j_m!} \prod_{s=0}^{m} (a_s x^s)^{j_s} \not\equiv F(x^p) \pmod{p^2},$$

где $a_m = e$, A — *множество всех упорядоченных наборов* $(j_0, \ldots, j_m)$ *чисел из* $\{0, 1, \ldots, p-1\}$ *таких, что*

$$j_0 + \cdots + j_m = p,\ j_1 + 2j_2 + \cdots + mj_m \equiv 0 \pmod{p}.$$

Ниже этот критерий будет перенесен на случай многочлена Галуа над кольцом Галуа $R = GR(q^n, p^n)$, $q = p^r$, $r \geqslant 2$, $n > 1$, $p \geqslant 3$.

Кроме того, в [11, § 4], [12, § 17] предложен следующий практический способ построения многочлена максимального периода над кольцом $R = GR(q^n, 2^n)$, $q = 2^r$.

Теорема 1.4 (см. [7, 12]). *Пусть* $G(x) \in R[x]$ — *унитарный многочлен степени* m *такой, что* $\mathrm{T}(\bar{G}) = q^m - 1$. *Определим рекуррентно следующие полиномы*: $G^{[0]}(x) = G(x)$, *и если* $G^{[k]}(x) = G_0^{[k]}(x^2) + xG_1^{[k]}(x^2)$, *то*

$$G^{[k+1]}(x) = (-1)^m (G_0^{[k]}(x)^2 - xG_1^{[k]}(x)^2).$$

Тогда произвольный полином вида

$$F(x) = G^{[r]}(x) + 2\Delta(x),$$

где полином $\Delta(x)$ *удовлетворяет условиям*

$$\deg \Delta(x) < m, \quad \bar{\Delta}(x) \neq \bar{0}, \quad \bar{\Delta}(x) \not\equiv x\bar{G}(x)' \pmod{\bar{G}(x)} \quad \textit{при } p = 2 < n,$$

есть многочлен максимального периода.

Ниже предлагается аналогичный способ построения отмеченного многочлена (а, следовательно, и многочлена максимального периода) над кольцом Галуа характеристики, отличной от 2^n.

Отметим еще раз, что всюду далее мы считаем, что $p \geqslant 3$.

2. Построение отмеченных многочленов

Как видно на примере теоремы 1.4, построение отмеченного многочлена $H(x)$, соответствующего данному регулярному многочлену Галуа $G(x)$ над собственным кольцом Галуа характеристики p^n с полем вычетов $GF(q)$, связано с построением некоторой последовательности многочленов, которая сходится за фиксированное число шагов к искомому отмеченному многочлену. При этом результаты работы [6] показывают, что в случае $p \geqslant 3$ эта задача, в свою очередь, связана с построением расширения T исходного кольца R, содержащего *первообразный* корень степени q из единицы.

Первообразным корнем степени q из единицы мы называем такой элемент α, для которого имеет место равенство:

$$x^q - e = \prod_{k=0}^{q-1} (x - \alpha^k), \tag{1}$$

причем $\alpha^i \neq \alpha^j$ при $0 \leqslant i < j \leqslant q-1$.

При этомб в отличие от случая поля нулевой характеристики, мы не предполагаем, что элемент $\alpha^i - \alpha^j$, $0 \leqslant i < j \leqslant q-1$, является обратимым. Элемент, удовлетворяющий соотношению (1) и последнему условию, будем называть *примитивным* корнем степени q из единицы.

Далее, поскольку указанное расширение T строится, вообще говоря, в классе колец Галуа—Эйзенштейна, то нам следует привести необходимые определения и факты.

Кольцом Галуа—Эйзенштейна [10] называется конечное коммутативное примарное кольцо главных идеалов. Пусть R — кольцо Галуа—Эйзенштейна, единственный максимальный идеал которого мы обозначим через $\mathfrak{p}_R$. Пусть $n_R = \operatorname{ind}\mathfrak{p}_R$ — индекс нильпотентности идеала $\mathfrak{p}_R$, $\bar{R} = R/\mathfrak{p}_R = GF(q)$, $q = p^r$, $\operatorname{char} R = p^d$. Пусть

$$Q_p = \left\{ \sum_{i\in\mathbb{Z}} c_i p^i \;\middle|\; c_i \in \mathbb{Z}_p \right\}$$

— p-адическое рациональное числовое поле,

$$Z_p = \left\{ \sum_{i\geqslant 0} c_i p^i \;\middle|\; c_i \in \mathbb{Z}_p \right\}$$

— кольцо p-адических целых чисел, $\mathscr{K}$ — алгебраическое замыкание поля Q_p.

Произвольное конечное расширение K поля Q_p в поле $\mathscr{K}$ называется p-адическим числовым полем, подкольцо Z_K поля K, состоящее из целых над Z_p элементов, называется кольцом целых чисел поля K [2]. Напомним, что элемент называется *целым* над Z_p, если он является корнем многочлена над кольцом Z_p.

Известно, что кольцо Z_K является дискретно нормированным и, следовательно, имеет единственный максимальный идеал $\mathfrak{p}_K$ [2]. Кроме того, кольцо Z_K является кольцом главных идеалов.

Если S, T — два коммутативных локальных цепных кольца с единицей таких, что кольцо T является расширением кольца S, то через $\mathrm{e}(T|S)$ обозначается *индекс ветвления* кольца T над кольцом S, т.е. натуральное число, для которого имеет место равенство: $\mathfrak{p}_S \cdot T = \mathfrak{p}_T^{\mathrm{e}(T|S)}$. Если $\mathrm{e}(T|S) = 1$, то кольцо T называется *неразветвленным* расширением кольца S.

Если K, L — два p-адических числовых поля, причем $K < L$, то через $\mathrm{e}(L|K)$ обозначается индекс ветвления кольца Z_L над кольцом Z_K. Через $f(L|K)$ обозначается степень поля классов вычетов L над K, т.е. степень расширения поля вычетов $\bar{Z}_L = Z_L/\mathfrak{p}_L$ над полем вычетов $\bar{Z}_K = Z_K/\mathfrak{p}_K$.

В [10] доказано, что кольцо Галуа—Эйзенштейна R изоморфно факторкольцу кольца целых чисел некоторого p-адического числового поля, а именно, существует поле K, являющееся элементом башни полей $Q_p < K < \mathscr{K}$, такое, что

$$R \cong Z_K/\mathfrak{p}_K^{\mathrm{n}_R}.$$

Лемма 2.1 (лемма Гензеля, [3,4])**.** *Пусть R — конечное коммутативное локальное кольцо с единицей e, $\mathfrak{p}_R$ — его максимальный идеал, $\bar{R} = R/\mathfrak{p}_R = GF(q)$ — поле вычетов кольца R. Если $F(x), G_0(x), H_0(x)$ — унитарные многочлены над кольцом R такие, что*

$$\bar{F}(x) = \bar{G}_0(x) \cdot \bar{H}_0(x), \quad (\bar{G}_0(x), \bar{H}_0(x)) = \bar{e},$$

то существует единственная пара унитарных многочленов $G(x), H(x) \in R[x]$ таких, что

$$F(x) = G(x) \cdot H(x), \quad \bar{G}(x) = \bar{G}_0(x), \quad \bar{H}(x) = \bar{H}_0(x).$$

Через $\mathscr{K}_{e,f}(K)$ обозначается класс всех конечных расширений L поля K в поле $\mathscr{K}$, для которых $e(L|K) = e$ и $f(L|K) = f$. Множество $\mathscr{G}_{K,f}(x)$ есть множество всех многочленов Галуа степени f из $Z_K[x]$ (т.е. множество всех таких унитарных многочленов $G(x)$ степени f над кольцом Z_K,

образы которых $\bar{G}(x)$ неприводимы над полем $\bar{Z}_K = Z_K/\mathfrak{p}_K$. Для произвольного $G(x) \in \mathscr{G}_{K,f}(x)$ множество $\mathscr{E}_{K,e}(G(x))$ есть множество всех многочленов Галуа—Эйзенштейна вида

$$E(x) = G(x)^e + E_{e-1}(x)G(x)^{e-1} + \cdots + E_0(x),$$

где $E_i \in \mathfrak{p}_K[x]$, $i = \overline{0, e-1}$, $E_0(x) \notin \mathfrak{p}_K^2[x]$, и степени многочленов $E_i(x)$ строго меньше f. Справедливо следующее утверждение.

Утверждение 2.2 (см. [10]). *Пусть $L \in \mathscr{K}_{e,f}(K)$ — расширение, порожденное корнем ξ некоторого унитарного неприводимого многочлена $F(x) \in Z_K[x]$. Равенство $Z_L = Z_K[\xi]$ выполнено тогда и только тогда, когда для некоторого $G(x) \in \mathscr{G}_{K,f}(x)$ многочлен $F(x)$ лежит в $\mathscr{E}_{K,e}(G(x))$.*

Следующая лемма была впервые получена А. С. Кузьминым (см., например, [5,6,12]) для случая примарных колец вычетов. Ниже мы обобщим этот результат на случай произвольного кольца Галуа—Эйзенштейна.

Лемма 2.3. *Пусть R — кольцо Галуа—Эйзенштейна, $G(x)$ — многочлен Галуа степени m над ним. Тогда существует башня колец Галуа—Эйзенштейна $R < S < T$ такая, что S — неразветвленное расширение кольца R, над которым многочлен $G(x)$ раскладывается на линейные множители, а в кольце T есть элемент α, являющийся первообразным корнем степени q из единицы, т.е. такой, что для него выполнено соотношение* (1).

Доказательство. Пусть $R = Z_K/\mathfrak{p}_K^{n_R}$, где K, Z_K и n_R определены выше. Пусть унитарный многочлен $\mathfrak{G}(x) \in Z_K[x]$ выбран так, что его образ в $Z_K/\mathfrak{p}_K^{n_R}[x]$ есть $G(x)$. Легко видеть, что тогда $\bar{\mathfrak{G}}(x)$ неприводим над $Z_K/\mathfrak{p}_K \cong R/\mathfrak{p}_R$.

Рассмотрим расширение L поля K в $\mathscr{K}$, порожденное корнем ξ многочлена $\mathfrak{G}(x)$. В соответствии с [10] имеем, что $\mathfrak{G}(x) \in \mathscr{G}_{K,m}[x]$ и $\mathfrak{G}(x) \in \mathscr{E}_{K,1}(\mathfrak{G}(x))$, откуда, согласно [10], L — неразветвленное расширение степени m поля K и $Z_L = Z_K[\xi]$.

Положим $Z_L/\mathfrak{p}_L^{n_R}$. Тогда S — неразветвленное расширение Галуа—Эйзенштейна кольца R степени $m = \deg \mathfrak{G}(x) = \deg G(x)$. Так как $\bar{S}$ — минимальное поле разложения неприводимого многочлена $\bar{G}(x)$ степени m, в $\bar{S}$ лежат его корни $\bar{\beta}_1, \ldots, \bar{\beta}_m$. Следовательно, в силу того, что лемма Гензеля справедлива для колец Галуа—Эйзенштейна, в кольце S лежат все корни $\beta_1, \ldots, \beta_m$ многочлена $G(x)$.

Пусть, далее, M — минимальное поле разложения многочлена $x^q - e$ над полем L. Так как $\operatorname{char} M = 0$, то в поле M лежит примитивный корень δ степени q из единицы. Очевидно, что $\delta \in Z_M$. Теперь, полагая

$$T = Z_M/\mathfrak{p}_M^{n_R \cdot \mathrm{e}(M|L)},$$

получаем необходимое нам расширение. В завершение отметим, что элемент α определяется как образ элемента δ при приведении по модулю идеала $\mathfrak{p}_M^{n_R \cdot e(M|L)}$.

В самом деле, обозначим через $\tilde{\beta}$ образ элемента $\beta \in Z_M$ в кольце $T = Z_M/\mathfrak{p}_M^{n_R \cdot e(M|L)}$. Поскольку элемент δ является примитивным корнем степени q из единицы, то справедливо равенство

$$x^q - e = \prod_{k=0}^{q-1}(x - \delta^k).$$

Приводя по модулю $\mathfrak{p}_M^{n_R \cdot e(M|L)}$ обе части этого равенства, получим

$$x^q - \tilde{e} = \prod_{k=0}^{q-1}(x - \tilde{\delta}^k).$$

Кроме того, поскольку δ — примитивный корень степени q из единицы, то элементы α^k, $k = \overline{0, q-1}$, попарно различны. Таким образом, справедливо соотношение (1). □

Лемма 2.4. *Пусть $R = GR(q^n, p^n)$ — кольцо Галуа, $G(x) \in R[x]$, T — описанное в лемме* 2.3 *расширение Галуа—Эйзенштейна кольца R, в котором имеется первообразный корень α степени q из единицы. Тогда имеет место включение*

$$\prod_{k=0}^{q-1} G\left(x\alpha^k\right) \in R[x].$$

Более того, если многочлен $G(x)$ раскладывается над R на линейные множители, т.е.

$$G(x) = \prod_{j=1}^{m}(x - \beta_j),$$

то имеет место равенство

$$\prod_{k=0}^{q-1} G\left(x\alpha^k\right) = \prod_{j=1}^{m}\left(x^q - \beta_j^q\right).$$

Доказательство. Рассмотрим многочлен от переменных $y_0, \ldots, y_{q-1}$ вида $\prod\limits_{k=0}^{q-1} G(xy_k)$. Этот многочлен является симметрическим над кольцом $R[x]$ от указанных переменных. Согласно основной теореме о симметрических многочленах найдется многочлен

$$\Psi(z_1, \ldots, z_q) \in R[x][z_1, \ldots, z_q]$$

такой, что

$$\prod_{k=0}^{q-1} G\left(xy_k\right) = \Psi\left(\sigma_1(y_0, \ldots, y_{q-1}), \ldots, \sigma_q(y_0, \ldots, y_{q-1})\right),$$

где $\sigma_1, \ldots, \sigma_q$ — элементарные симметрические функции от q переменных. Поскольку из (1), согласно формулам Виета, следуют равенства

$$\sigma_1(e, \alpha, \ldots, \alpha^{q-1}) = \cdots = \sigma_{q-1}(e, \alpha, \ldots, \alpha^{q-1}) = 0, \quad \sigma_q(e, \alpha, \ldots, \alpha^{q-1}) = e,$$

имеем

$$\prod_{k=0}^{q-1} G\left(x\alpha^k\right) = \Psi(0, \ldots, 0, e) \in R[x].$$

Пусть теперь $G(x) = \prod\limits_{j=1}^{m}(x - \beta_j)$. Тогда

$$\prod_{k=0}^{q-1} G\left(x\alpha^k\right) = \prod_{k=0}^{q-1}\prod_{j=1}^{m}\left(x\alpha^k - \beta_j\right) = \prod_{j=1}^{m}\prod_{k=0}^{q-1}\left(x\alpha^k - \beta_j\right) = \prod_{j=1}^{m}\left(x^q - \beta_j^q\right),$$

так как все q-местные симметрические функции от $e, \alpha, \ldots, \alpha^{q-1}$ равны нулю вплоть до σ_{q-1}, и функция σ_q от $e, \alpha, \ldots, \alpha^{q-1}$ равна e. □

Теорема 2.5. *Пусть $R = GR(q^n, p^n)$, $q = p^r$, — произвольное кольцо Галуа, $G(x) \in R[x]$ — регулярный многочлен Галуа, кольца S, T и элемент α описаны в лемме* 2.3. *Тогда многочлен $G(x)$ является отмеченным в том и только в том случае, когда*

$$G(x^q) = \prod_{k=0}^{q-1} G\left(x\alpha^k\right).$$

Доказательство. Заметим, что $\mathrm{T}(G(x)) = \operatorname{ord}\beta$, где β — произвольный корень $G(x)$ в кольце S. Пусть $\beta_1, \ldots, \beta_m$ — все корни $G(x)$ в кольце S. В соответствии с леммой 2.4 выполнены следующие соотношения:

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \prod_{j=1}^{m}(x^q - \beta_j^q) \in R[x].$$

Пусть $G(x)$ — отмеченный многочлен. Тогда $\mathrm{T}(G(x)) = \mathrm{T}(\bar{G}(x)) = \tau$. При этом для каждого $j \in \overline{1,m}$ имеем $\operatorname{ord}\beta_j = \operatorname{ord}\bar{\beta}_j = \tau$ (см. [11]). Поскольку $G(x)$ — многочлен Галуа, то числа q и τ взаимно просты. Согласно лемме 2.4 многочлен $H(x) = \prod\limits_{j=1}^{m}\left(x - \beta_j^q\right)$ лежит в $R[x]$. Кроме того, поскольку $\bar{\beta}_j \in \bar{R} = GF(q)$, имеем $\bar{\beta}_j^q = \bar{\beta}_j$, $j = \overline{1,m}$. Следовательно,

$$\bar{H}(x) = \prod_{j=1}^{m}\left(x - \bar{\beta}_j^q\right) = \prod_{j=1}^{m}\left(x - \bar{\beta}_j\right) = \bar{G}(x),$$

т.е.

$$G(x) \equiv H(x) \pmod{J(R)}.$$

Так как

$$\mathrm{T}(G(x)) = \mathrm{T}(\bar{G}(x)) = \operatorname{ord}\beta_1 = \tau, \quad \mathrm{T}\left(H(x)\right) = \operatorname{ord}\beta_1^q = \frac{\operatorname{ord}\beta_1}{(\tau,q)} = \operatorname{ord}\beta_1,$$

то $H(x)$ — отмеченный многочлен. Согласно [11], для данного регулярного сепарабельного многочлена над кольцом R имеется единственный отмеченный многочлен, сравнимый с ним по модулю радикала Джекобсона. Следовательно, $G(x) = H(x)$ или

$$G(x^q) = H(x^q) = \prod_{j=1}^{m}\left(x^q - \beta_j^q\right) = \prod_{k=0}^{q-1} G\left(x\alpha^k\right).$$

Обратно, если

$$G(x^q) = \prod_{k=0}^{q-1} G\left(x\alpha^k\right),$$

то согласно лемме 2.4

$$G(x) = H(x) = \prod_{j=1}^{m}\left(x - \beta_j^q\right).$$

Поскольку период регулярного многочлена Галуа совпадает с порядком любого из его корней в минимальном кольце разложения, а также поскольку периоды многочленов в левой и правой частях предыдущего равенства совпадают, то $\operatorname{ord}\beta_1 = \operatorname{ord}\beta_1^q$, откуда $(\operatorname{ord}\beta_1, q) = 1$. Так как

$$\operatorname{ord}\bar{\beta}_1 \mid \operatorname{ord}\beta_1 \mid \operatorname{ord}\bar{\beta}_1 \cdot p^{n-1}$$

(см. [11]), то $\operatorname{ord}\beta_1 = \operatorname{ord}\bar{\beta}_1$, что, в свою очередь, влечет равенство периодов многочленов $G(x)$ и $\bar{G}(x)$, т.е. многочлен $G(x)$ — отмеченный. □

Рассмотрим последовательность $H_0(x), H_1(x), \ldots$ многочленов степени m над кольцом R, получаемых рекурсивно согласно правилу

$$H_0(x) = G(x), \quad H_{i+1}(x^q) = \prod_{k=0}^{q-1} H_i\left(x\alpha^k\right), \quad i = \overline{0,n-2}, \tag{2}$$

где элемент α описан в лемме 2.3. Согласно лемме 2.4 многочлен $\prod\limits_{k=0}^{q-1} H_i(x\alpha^k)$ принадлежит кольцу $R[x]$ и, кроме того, многочлен $\prod\limits_{k=0}^{q-1} H_i(x\alpha^k)$ является многочленом от x^q. Следовательно, выписанное выше правило (2) позволяет корректно строить многочлены над кольцом R степени m.

Лемма 2.6. *Если* $G(x) = \prod\limits_{j=1}^{m}(x - \beta_j)$, *то для каждого* $i \in \overline{0,n-2}$ *имеем*

$$H_i(x) = \prod_{j=1}^{m}\left(x - {\beta_j}^{q^i}\right).$$

Доказательство. Справедливость леммы при $i = 0$ проверяется непосредственно. Предположим, что при всех $k \in \overline{0,i}$ утверждение леммы относительно многочлена $H_k(x)$ выполнено. Тогда, используя лемму 2.4, получаем

$$H_{i+1}(x^q) = \prod_{k=0}^{q-1} H_i(x\alpha^k) = \prod_{j=1}^{m}(x^q - \beta_j^{q^{i+1}}),$$

поскольку, по предположению индукции, ${\beta_1}^{q^i}, \ldots, {\beta_m}^{q^i}$ — все корни многочлена $H_i(x)$. □

Пусть K — произвольное коммутативное локальное кольцо с единицей, $J(K)$ — радикал Джекобсона этого кольца. При $i \leqslant \operatorname{ind} J(K)$ обозначим через ϕ_i канонический эпиморфизм кольца K на его факторкольцо $K/J(K)^i$.

Пусть $R < S < T$ — указанная в лемме 2.3 башня колец. Тогда для любого $i \in \overline{1,n}$ видим, что $\phi_i(R) < \phi_i(S) < \phi_i(T)$ — башня колец, обладающая аналогичными свойствами, а именно, в кольце $\phi_i(S)$ многочлен $\phi_i(G)$ раскладывается на линейные множители, а в кольце $\phi_i(T)$ найдется элемент $\gamma_i = \phi_i(\alpha)$, являющийся первообразным корнем из единицы:

$$x^q - e = \prod_{j=0}^{q-1} \left(x - {\gamma_i}^j\right).$$

Кроме того, для любых $i, j \in \overline{0,n}$ образ $\overline{\phi_i(H_j(x))}$ многочлена $\phi_i(H_j(x))$ при приведении по модулю идеала $J(\phi_i(R))[x]$ совпадает с точностью до изоморфизма полей $\phi_i(R)/J(\phi_i(R))$ и $R/J(R)$ с образом $\bar{G}(x)$ многочлена $G(x)$ при приведении по модулю $J(R)[x]$.

Утверждение 2.7. *При любых значениях $i \in \overline{0,n-1}$ и $l \leqslant \min\{ri+1, n\}$ многочлен $\phi_l(H_i(x))$ является отмеченным над кольцом $\phi_l(R)$.*

Доказательство. Как известно,

$$\mathrm{T}\left(\phi_l(H_i(x))\right) \mid \mathrm{T}\left(\overline{\phi_l(H_i(x))}\right) \cdot p^{l-1} = \tau \cdot p^{l-1},$$

где $\tau = \mathrm{T}\left(\bar{G}(x)\right) = \operatorname{ord}\overline{\phi_l(\beta)} = \operatorname{ord}\bar{\beta}$, β — произвольный корень $G(x)$ в кольце S. С другой стороны,

$$\mathrm{T}\left(\phi_l(H_i(x))\right) = \operatorname{lcm}\{\operatorname{ord}\phi_l(\beta_j)^{q^i},\ j = \overline{1,m}\},$$

где $\beta_1, \ldots, \beta_m$ — все корни многочлена $G(x)$ в кольце S. Кроме того, для всех $j \in \overline{1,m}$ имеем $\operatorname{ord}\phi_l(\beta_j) \mid \tau p^{l-1}$, откуда, поскольку $\tau \mid \operatorname{ord}\phi_l(\beta_j)$ и $(\tau, q) = 1$, следует

$$\tau \mid \operatorname{ord}\phi_l(\beta_j)^{q^i} \mid \frac{\operatorname{ord}\phi_l(\beta_j)}{(q^i, \tau p^{l-1})} = \tau$$

при значениях l таких, что $l - 1 \leqslant ri$, $l \leqslant n$. Таким образом, при $l \leqslant \min\{ri+1, n\}$ имеем

$$\mathrm{T}\left(\phi_l(H_i(x))\right) = \mathrm{T}\left(\overline{\phi_l(H_i(x))}\right),$$

т.е. $\phi_l(H_i(x))$ — отмеченный над $\phi_l(R)$ многочлен. □

Следствие 2.8. *Если $F(x)$ — многочлен Галуа над кольцом $R = GR(q^n, p^n)$, $q = p^r$, $p \geqslant 3$, то последовательность многочленов $H_i(x)$, $i \in \mathbb{N}_0$, не более чем за $[n/r]$ шагов сходится к отмеченному многочлену, соответствующему многочлену $F(x)$.*

Доказательство. В обозначениях утверждения 2.7 следует заметить, что $R = \phi_n(R)$. □

3. Критерий полноты периода многочлена Галуа над собственным кольцом Галуа

Пусть $R = GR(q^n, p^n)$ — собственное кольцо Галуа, причем $p > 2$, $G(x)$ — многочлен Галуа над ним. Целью этого раздела является получение критерия полноты периода многочлена $G(x)$ в терминах коэффициентов этого многочлена.

Как показано А. А. Нечаевым, если $D(x) = \operatorname{rad} G(x)$ — отмеченный многочлен из $R[x]$, сравнимый с $G(x)$ по модулю $J(R)$, то остаток $\operatorname{Res}(D(x), G(x))$ при делении многочлена $D(x)$ на многочлен $G(x)$ имеет вид $p^\lambda W(x)$, $1 \leqslant \lambda \leqslant n$, $W(x) \not\equiv 0 \pmod{J(R)}$, и тогда $\mathrm{T}(G) = \mathrm{T}\left(\bar{G}\right) p^{n-\lambda}$. Отсюда следует, что $G(x)$ — многочлен полного периода тогда и только тогда, когда $\lambda = 1$.

Обозначим через $\tilde{R}$ кольцо Галуа $\phi_2(R) = R/J(R)^2 = GR(q^2, p^2)$.

Лемма 3.1. *$G(x)$ является многочленом полного периода над R тогда и только тогда, когда $\tilde{G}(x) = \phi_2(G(x))$ является многочленом полного периода над $\tilde{R}$.*

Таким образом, вопрос о полноте периода многочлена $G(x)$ сводится к нахождению $\operatorname{rad} \tilde{G}(x)$ над $\tilde{R}$. Поэтому далее считаем, что $R = GR(q^2, p^2)$, $q = p^r$, $r \geqslant 2$. Тогда в соответствии с утверждением 2.7 имеем $H_1(x) = \operatorname{rad} G(x)$. Поэтому в дальнейшем нас будет интересовать вид многочлена $H_1(x)$.

Теорема 3.2. *Пусть $R = GR(q^2, p^2)$, $q = p^r$, $r \geqslant 2$, $p \geqslant 3$, $G(x) = x^m + g_{m-1}x^{m-1} + \cdots + g_0$ — многочлен Галуа над кольцом Галуа R. Тогда имеет место равенство*

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \sum_{l=1}^{m+1} \sum_{(k_1,\ldots,k_l)\in\mathscr{X}_l} \sum_{(j_{k_1},\ldots,j_{k_l})\in\mathscr{Y}(\mathscr{X}_l)} \frac{p!}{\prod\limits_{s=1}^{l} j_{k_s}!} \prod_{s=1}^{l} \left(g_{k_s} x^{k_s}\right)^{j_{k_s} p^{r-1}}, \tag{3}$$

где элемент α описан в лемме 2.3, а множества $\mathscr{X}_l$ and $\mathscr{Y}(\mathscr{X}_l)$, $l = \overline{1, m+1}$, определены следующим образом:

$$\mathscr{X}_l = \left\{(k_1, \ldots, k_l) : 0 \leqslant k_1 < \ldots < k_l \leqslant m,\ k_i \equiv k_j \pmod q,\ i, j \in \overline{1, l}\right\},$$

$$\mathscr{Y}(\mathscr{X}_l) = \left\{(j_{k_1}, \ldots, j_{k_l}) : 0 < j_{k_s} \leqslant p,\ s \in \overline{1, l},\ \sum_{s=1}^{l} j_{k_s} = p\right\}.$$

Доказательство. Представим многочлен $G(x)$ в виде

$$G(x) = a_0(x^q) + xa_1(x^q) + \cdots + x^{q-1}a_{q-1}(x^q) \tag{4}$$

и при каждом $t \in \overline{0, q-1}$ положим $b_t(x) = x^t a_t(x^q)$. Здесь многочлены $x^t a_t(x^q)$, $t = \overline{0, q-1}$, получены путем группирования одночленов, степени которых сравнимы с t по модулю q. Пусть

$$a_t(x) = \sum_{s=0}^{u_t} a_{i_s(t)} x^{i_s(t)}.$$

Имеем:

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \prod_{k=0}^{q-1} \left(\sum_{t=0}^{q-1} x^t \alpha^{kt} a_t(x^q)\right) =$$

$$= \prod_{k=0}^{q-1} \left(\sum_{t=0}^{q-1} b_t(x)\alpha^{kt}\right) = \sum_{(j_0,\ldots,j_{q-1})\in\mathbb{Z}_q^{(q)}} b_{j_0}(x)\cdots b_{j_{q-1}}(x)\alpha^{\sum\limits_{k=0}^{q-1} kj_k}.$$

Возможны следующие случаи.

(1) $(j_0, \ldots, j_{q-1}) = t \cdot \vec{1}$. Каждый такой вектор встречается единственный раз, и для каждого из этих векторов

$$\alpha^{\sum\limits_{k=0}^{q-1} kj_k} = \alpha^{t\sum\limits_{k=0}^{q-1} k} = \alpha^{t\frac{q(q-1)}{2}} = e.$$

(2) $(j_0,\dots,j_{q-1}) \neq t\cdot\vec{1}$. Рассмотрим сумму по всем векторам $(j'_0,\dots,j'_{q-1})$, являющимся циклическим сдвигом вектора $(j_0,\dots,j_{q-1})$:

$$\sum b_{j'_0}(x)\cdots b_{j'_{q-1}}(x)\alpha^{\sum\limits_{k=0}^{q-1} kj'_k} = b_{j_0}(x)\cdots b_{j_{q-1}}(x)\sum_{r=0}^{q-1}\alpha^{\sum\limits_{k=0}^{q-1}(k+r)j_k} =$$

$$= b_{j_0}(x)\cdots b_{j_{q-1}}(x)\sum_{r=0}^{q-1}\alpha^{\sum\limits_{k=0}^{q-1} kj_k + r\sum\limits_{k=0}^{q-1} j_k} = b_{j_0}(x)\cdots b_{j_{q-1}}(x)\alpha^{\sum\limits_{k=0}^{q-1} kj_k}\sum_{r=0}^{q-1}\left(\alpha^{\sum\limits_{k=0}^{q-1} j_k}\right)^r =$$

$$= \begin{cases} 0, & \text{если } \sum\limits_{k=0}^{q-1} j_k \not\equiv 0 \pmod q, \\ qb_{j_0}(x)\cdots b_{j_{q-1}}(x)\alpha^{\sum\limits_{k=0}^{q-1} kj_k}, & \text{если } \sum\limits_{k=0}^{q-1} j_k \equiv 0 \pmod q. \end{cases}$$

Последнее равенство в цепочке имеет место, поскольку $\operatorname{ord}\alpha = q$.

Так как $\operatorname{char} R = p^2 \mid q$, имеем

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \sum_{t=0}^{q-1} b_t^q = \sum_{t=0}^{q-1} x^{qt} a_t(x^q)^q. \tag{5}$$

Таким образом, для того, чтобы найти многочлен $\prod\limits_{k=0}^{q-1} G(x\alpha^k)$, достаточно исследовать многочлены $a_t(x)^q$, $t = \overline{0,q-1}$.

Пусть теперь при некотором $t \in \overline{0,q-1}$ имеем $a_t(x) = a_{i_u(t)}x^{i_u(t)} + \dots + a_{i_0(t)}x^{i_0(t)}$. Рассмотрим многочлен

$$a_t(x^q)^q = \sum_{\substack{(c_0,\dots,c_u):\\ 0\leqslant c_s\leqslant q,\\ \sum\limits_{s=0}^{u} c_s = q}} \frac{q!}{\prod\limits_{s=0}^{u} c_s!}\prod_{s=0}^{u} a_{i_s(t)}^{c_s} x^{q\sum\limits_{s=0}^{u} i_s(t)c_s} =$$

$$= \sum_{s=0}^{u} a_{i_s(t)}^q x^{q^2 i_s(t)} + \sum_{\substack{(c_0,\dots,c_u):\\ 0\leqslant c_s< q,\\ \sum\limits_{s=0}^{u} c_s = q}} \frac{q!}{\prod\limits_{s=0}^{u} c_s!}\prod_{s=0}^{u} a_{i_s(t)}^{c_s} x^{q\sum\limits_{s=0}^{u} i_s(t)c_s}. \tag{6}$$

Обозначим через $\|w\|$, $w \in R\setminus\{0\}$, число $t \in \mathbb{N}_0$ такое, что $w \in J(R)^t \setminus J(R)^{t+1}$. Кроме того, $\|0\| = n$. Поскольку все вычисления мы проводим по модулю p^2, то в предыдущем многочлене нас будут интересовать только те мономы, про коэффициенты при которых нельзя сказать, что они заведомо равны нулю по модулю p^2.

Пусть $c_s = \sum\limits_{t=0}^{r-1} c_s^{(t)} p^t$. Известно [9, лемма 6.39], что

$$\|c_s!\| = \frac{c_s - \sum\limits_{t=0}^{r-1} c_s^{(t)}}{p-1}.$$

Согласно [1, лемма 15.576], соотношение

$$\left\| q!/\prod_{s=0}^{u} c_s! \right\| = 1$$

имеет место тогда и только тогда, когда

$$\sum_{s=0}^{u} c_s^{(r-1)} = p, \quad c_s^{(t)} = 0, \quad t \in \overline{0, r-2};$$

отсюда следует, что в сумме (6) останутся только слагаемые вида

$$a_t(x)^q = \sum_{s=0}^{u} a_{i_s(t)}^q x^{qi_s(t)} + \sum_{\substack{(c_0,\dots,c_u):0\leqslant c_s<p,\\ \sum\limits_{s=0}^{u} c_s=p}} \frac{q!}{\prod\limits_{s=0}^{u}(c_s p^{r-1})!} \prod_{s=0}^{u} (a_{i_s(t)} x^{i_s(t)})^{c_s p^{r-1}} =$$

$$= \sum_{s=0}^{u} a_{i_s(t)}^q x^{qi_s(t)} + \sum_{\substack{(c_0,\dots,c_u):0\leqslant c_s<p,\\ \sum\limits_{s=0}^{u} c_s=p}} \frac{p!}{\prod\limits_{s=0}^{u} c_s!} \prod_{s=0}^{u} (a_{i_s(t)} x^{i_s(t)})^{c_s p^{r-1}} =$$

$$= \sum_{\substack{(c_0,\dots,c_u):0\leqslant c_s\leqslant p,\\ \sum\limits_{s=0}^{u} c_s=p}} \frac{p!}{\prod\limits_{s=0}^{u} c_s!} \prod_{s=0}^{u} (a_{i_s(t)} x^{i_s(t)})^{c_s p^{r-1}} = \left(\sum_{s=0}^{u} (a_{i_s(t)} x^{i_s(t)})^{p^{r-1}} \right)^p. \quad (7)$$

Здесь мы во втором переходе воспользовались известной теоремой Люка для полиномиальных коэффициентов [1, теорема 4.7.1], [8, лемма 1(b)]. Подставляя полученные соотношения в формулу (5), получим:

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \sum_{t=0}^{q-1} x^{qt} \sum_{\substack{(c_{0,t},\dots,c_{u_t,t}):\\ 0\leqslant c_{s,t}\leqslant p,\\ \sum\limits_{s=0}^{u_t} c_{s,t}=p}} \frac{p!}{\prod_{s=0}^{u_t} c_{s,t}!} \prod_{s=0}^{u_t} (a_{i_s(t)} x^{qi_s(t)})^{c_{s,t} p^{r-1}} =$$

$$= \sum_{t=0}^{q-1} \sum_{\substack{(c_{0,t},\dots,c_{u_t,t}):\\ 0\leqslant c_{s,t}\leqslant p,\\ \sum\limits_{s=0}^{u_t} c_{s,t}=p}} \frac{p!}{\prod_{s=0}^{u_t} c_{s,t}!} \prod_{s=0}^{u_t} (a_{i_s(t)} x^{t+qi_s(t)})^{c_{s,t} p^{r-1}}. \quad (8)$$

Заметим, что, по определению многочлена $a_t(x)$, согласно (6), при всех $t = \overline{0, q-1}$, $s = \overline{0, u_t}$ число $k_s = t + qi_s(t) \in \overline{0, m}$ есть не что иное, как степень, в которой переменная x входит в многочлен $G(x)$, а элемент $a_{i_s(t)}$ кольца R есть не что иное, как коэффициент при x^{k_s} в многочлене $G(x)$. Для $k_s = t + qi_s(t)$ положим $g_{k_s} = a_{i_s(t)}$, $j_{k_s} = c_{s,t}$. Такое обозначение корректно, поскольку по k_s параметр t определяется однозначно. Теперь, производя замену переменных и меняя порядок суммирования, получим искомое равенство:

$$\prod_{k=0}^{q-1} G(x\alpha^k)) = \sum_{l=1}^{m+1} \sum_{\vec{k}\in\mathscr{X}_l} \sum_{\vec{j}\in\mathscr{Y}(\mathscr{X}_l)} \frac{p!}{\prod\limits_{s=1}^{l} j_{k_s}!} \prod_{s=1}^{l} \left(g_{k_s} x^{k_s} \right)^{j_{k_s} p^{r-1}}.$$

Теорема доказана. □

Следствие 3.3. *Пусть $R = GR(q^n, p^n)$, $n \geqslant 2$, $q = p^r$, $r \geqslant 2$, $p \geqslant 3$ — собственное кольцо Галуа, $G(x)$ — регулярный многочлен Галуа над R. Многочлен $G(x)$ является многочленом полного*

периода тогда и только тогда, когда

$$G(x^q) \not\equiv \sum_{l=1}^{m+1} \sum_{\vec{k}\in\mathscr{X}_l} \sum_{\vec{j}\in\mathscr{Y}(\mathscr{X}_l)} \frac{p!}{\prod\limits_{s=1}^{l} j_{k_s}!} \prod_{s=1}^{l} \left(g_{k_s} x^{k_s}\right)^{j_{k_s} p^{r-1}} \pmod{J^2(R)}, \tag{9}$$

где

$$\mathscr{X}_l = \{(k_1,\ldots,k_l) : 0 \leqslant k_1 < \ldots < k_l \leqslant m,\ k_i \equiv k_j \pmod q,\ i,j \in \overline{1,l}\},$$

$$\mathscr{Y}(\mathscr{X}_l) = \{(j_{k_1},\ldots,j_{k_l}) : 0 < j_{k_s} \leqslant p,\ s \in \overline{1,l},\ \sum_{s=1}^{l} j_{k_s} = p\}.$$

Доказательство. Как видно из леммы 3.1, полноту периода многочлена $G(x)$ достаточно исследовать по модулю $J^2(R) = p^2R$. При этом согласно теореме 2.5 $G(x)$ — многочлен полного периода тогда и только тогда, когда

$$G(x^q) \not\equiv \prod_{k=0}^{q-1} G(x\alpha^k) \pmod{p^2R}.$$

Кроме того, согласно теореме 3.2

$$\prod_{k=0}^{q-1} G(x\alpha^k) \equiv \sum_{l=1}^{m+1} \sum_{\vec{k}\in\mathscr{X}_l} \sum_{\vec{j}\in\mathscr{Y}(\mathscr{X}_l)} \frac{p!}{\prod\limits_{s=1}^{l} j_{k_s}!} \prod_{s=1}^{l} \left(g_{k_s} x^{k_s}\right)^{j_{k_s} p^{r-1}} \pmod{p^2R}.$$

Из всего вышесказанного легко вытекает утверждение следствия 3.3. □

Замечание 3.4. Полезно заметить, что правые части равенств (3) и (9) равны

$$\sum_{t=0}^{q-1} \left(\sum_{k\equiv t \pmod q} (g_k x^k)^{p^{r-1}} \right)^p. \tag{10}$$

В самом деле, из (7) и из представлений (4) и (5) получаем, что

$$\prod_{k=0}^{q-1} G(x\alpha^k) = \sum_{t=0}^{q-1} x^{qt} \left(\sum_{s=0}^{u} (a_{i_s(t)} x^{qi_s(t)})^{p^{r-1}} \right)^p =$$

$$= \sum_{t=0}^{q-1} \left(\sum_{s=0}^{u} (a_{i_s(t)} x^{qi_s(t)+t})^{p^{r-1}} \right)^p = \sum_{t=0}^{q-1} \left(\sum_{k\equiv t \pmod q} (g_k x^k)^{p^{r-1}} \right)^p.$$

Таким образом, критерий предыдущей леммы может быть сформулирован следующим образом: многочлен $G(x) = x^m + \sum\limits_{j=0}^{m-1} g_j x^j$ над собственным кольцом Галуа $R = GR(q^n, p^n)$ нечетной характеристики является многочленом максимального периода тогда и только тогда, когда

$$G(x^q) \not\equiv \sum_{t=0}^{q-1} \left(\sum_{k\equiv t \pmod q} (g_k x^k)^{p^{r-1}} \right)^p \pmod{p^2R[x]}. \tag{11}$$

Такая форма критерия более привлекательна в силу своей компактности, но менее удобна с практической точки зрения, нежели чем представление (9).

СПИСОК ЛИТЕРАТУРЫ

1. *Берлекэмп Э. Р.* Алгебраическая теория кодирования. — М.: Мир, 1971.
2. *Боревич З. И., Шафаревич И. Р.* Теория чисел. — М: Наука, 1964.
3. *Бурбаки Н.* Коммутативная алгебра. — М.: Мир, 1971.
4. *Зарисский О., Самюэль П.* Коммутативная алгебра. — М.: ИЛ, 1963.
5. *Кузьмин А. С.* Многочлены максимального периода над кольцами вычетов целых чисел// Тр. III Междунар. конф. по алгебре. Красноярск, 23–28 авг. 1993 г./ Тез. докл. — С. 192.
6. *Кузьмин А. С.* Многочлены максимального периода над примарными кольцами вычетов// Фундам. прикл. мат. — 1995 — *1*, № 2. — С. 549–551.
7. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности// Тр. дискр. мат. — 1997. — *1*. — С. 139–202.
8. *Куракин В. Л.* Представления над кольцом $\mathbb{Z}_{p^n}$ линейной рекуррентной последовательности максимального периода над полем $GF(p)$// Дискр. мат. — 1992. — *4*, № 4. — С. 96–116.
9. *Лидл Р., Нидеррайтер Г.* Конечные поля. — М.: Мир, 1988.
10. *Нечаев А. А.* О строении конечных колец// Мат. заметки. — 1971. — *10*, № 6. — С. 679–688.
11. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами// Мат. сб. — 1993. — *184*, № 4. — С. 21–56.
12. *Kuzmin A. S., Kurakin V. L., Mikhalev A. V., Nechaev A. A.* Linear recurrences over rings and modules// J. Math. Sci. — 1995. — *76*, № 6. — С. 2793–2915.
13. *McDonald C.* Finite rings with identity. — N.Y.: Marcel Dekker, 1974.
14. *Radghavendran R.* A class of finite rings// Compos. Math. — 1970. — *22*, № 1. — С. 49–57.

В. Н. Цыпышев
E-mail: tsypyschev@yandex.ru

Современная математика и ее приложения. Том 14 (2004). С. 121–127

УДК 512.54

ОБ АФФИННО ЗАМКНУТЫХ ОДНОРОДНЫХ ПРОСТРАНСТВАХ

© 2004 г. **И. В. АРЖАНЦЕВ, Н. А. ТЕННОВА**

Аннотация. Для произвольной алгебраической группы G получено конструктивное описание аффинно замкнутых однородных пространств G/H, т.е. аффинных однородных пространств, допускающих лишь тривиальное аффинное вложение. Охарактеризованы аффинные G-алгебры, каждая инвариантная подалгебра которых конечно порождена.

СОДЕРЖАНИЕ

1. Введение

Пусть G — аффинная алгебраическая группа над алгебраически замкнутым полем $\mathbb{K}$ нулевой характеристики и H — алгебраическая подгруппа в G. Согласно теореме Шевалле однородное пространство G/H обладает канонической структурой квазипроективного многообразия. *Вложением* однородного пространства G/H называют алгебраическое G-многообразие X с отмеченной точкой $x \in X$ такой что орбита Gx плотна (и открыта) в X и стабилизатор G_x совпадает с H. Будем обозначать вложение символом $G/H \hookrightarrow X$. Говорят, что вложение *тривиально*, если $Gx = X$. Вложение $G/H \hookrightarrow X$ называют *аффинным*, если многообразие X аффинно. Нетрудно показать (см. например, [1]), что пространство G/H допускает аффинное вложение тогда и только тогда, когда G/H является квазиаффинным многообразием или, эквивалентно, H реализуется как стабилизатор вектора в конечномерном G-модуле. В этой ситуации подгруппа H называется *обозримой* в G. Конструктивное описание обозримых подгрупп в произвольной алгебраической группе G получено в [3].

Определение 1 (см. [6])**.** Однородное пространство G/H называется *аффинно замкнутым*, если оно допускает лишь тривиальное аффинное вложение.

Аффинно замкнутое однородное пространство автоматически аффинно. Изучение этого класса однородных пространств мотивировано желанием гарантировать замкнутость G-орбиты на аффинном многообразии, зная лишь стабилизатор некоторой точки этой орбиты.

Для редуктивной группы G однородное пространство G/H является аффинным многообразием тогда и только тогда, когда подгруппа H редуктивна (критерий Мацусимы). Отметим, что для произвольной алгебраической группы G описание аффинных однородных пространств G/H в групповых терминах для пары (G, H) является открытой проблемой, обсуждение которой можно найти в [9, Chap. 2].

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект МАС 03-01-06252), CRDF RM1-2543-MO-03 и гранта Президента Российской Федерации МК-1279.2004.1.

В случае редуктивной группы G описание аффинно замкнутых пространств непосредственно следует из результатов Д. Луны [11].

Теорема 1. *Пусть группа G редуктивна. Однородное пространство G/H аффинно замкнуто тогда и только тогда, когда подгруппа H редуктивна и имеет конечный индекс в своем нормализаторе $N_G(H)$. Более того, если G действует на аффинном многообразии X и стабилизатор точки $x \in X$ содержит редуктивную подгруппу H, для которой группа $N_G(H)/H$ конечна, то орбита Gx замкнута.*

Например, для максимального тора T редуктивной группы G группа Вейля $W = N_G(T)/T$ конечна и потому G/T аффинно замкнуто. Если $\rho : H \to SL(V)$ — неприводимое представление полупростой группы, то пространство $SL(V)/\rho(H)$ аффинно замкнуто, поскольку согласно лемме Шура группа $N_{SL(V)}(\rho(H))/\rho(H)$ конечна. Таким образом, класс аффинно замкнутых однородных пространств достаточно широк.

В [5] аффинно замкнутые однородные пространства редуктивной группы G играли ключевую роль при классификации аффинных G-алгебр, каждая инвариантная подалгебра которых конечно порождена. Характеризации комплексных аффинно замкнутых пространств редуктивных групп в терминах компактных групп преобразований и инвариантных алгебр на компактных однородных пространствах даны в [10] и [8].

Цель настоящей работы — обобщить результат Д. Луны на случай произвольной алгебраической группы G (теорема 2) и получить классификацию аффинных G-алгебр с конечно порожденными инвариантными подалгебрами (теорема 3). Отметим, что случай разрешимой G над алгебраически замкнутым полем произвольной характеристики разобран в [4].

2. Описание аффинно замкнутых пространств

Зафиксируем разложение Леви $G = LG^u$ группы G в полупрямое произведение редуктивной подгруппы L и унипотентного радикала G^u. Обозначим через ϕ гомоморфизм факторизации $\phi : G \to G/G^u$, образ которого естественно отождествляется с L, и пусть $K = \phi(H)$.

Теорема 2. *Следующие условия эквивалентны*:

1) *G/H аффинно замкнуто*;
2) *L/K аффинно замкнуто.*

Заметим, что обозримость подгруппы H в группе G равносильна обозримости K в L (см. [3], [9, Theorem 7.3]).

Предположим, что L/K допускает нетривиальное аффинное вложение. Тогда найдется L-модуль V и точка $v \in V$, стабилизатор L_v которой совпадает с K и граница орбиты $Y = Z \setminus Lv$, где $Z = \overline{Lv}$, непуста. Пусть $I(Y)$ — идеал в $\mathbb{K}[Z]$, определяющий подмногообразие Y. Напомним, что для произвольного действия алгебраической группы G на аффинном многообразии X каждый элемент $f \in \mathbb{K}[X]$ лежит в конечномерном инвариантном подпространстве или, эквивалентно, $\mathbb{K}[X]$ есть сумма своих конечномерных G-подмодулей. Поэтому найдется конечномерный L-подмодуль $V_1 \subset I(Y)$, порождающий $I(Y)$ как идеал. Включение $V_1 \subset \mathbb{K}[Z]$ определяет L-эквивариантный морфизм $\psi : Z \to V_1^*$, причем $\psi^{-1}(0) = Y$. Тогда L-эквивариантный морфизм

$$\xi : Z \to V_2 = V_1^* \oplus V \otimes V_1^*, \quad z \to (\psi(z), z \otimes \psi(z)),$$

отображает Y в нуль и инъективен на открытой орбите в Z. Тем самым построено вложение L/K в L-модуль V_2, замыкание образа которого содержит нуль. Пусть $v_2 = \xi(v)$. Согласно критерию Гильберта—Мамфорда найдется однопараметрическая подгруппа $\lambda : \mathbb{K}^* \to L$ такая, что $\lim\limits_{t\to 0} \lambda(t)v_2 = 0$. Рассмотрим весовое разложение $v_2 = v_2^{(i_1)} + \cdots + v_2^{(i_s)}$ вектора v_2, где $\lambda(t)v_2^{(i_k)} = t^{i_k}v_2^{(i_k)}$ и все i_k положительны.

Учитывая отождествление $G/G^u = L$, можно рассматривать V_2 как G-модуль. Пусть W — конечномерный G-модуль, в котором имеется вектор w со стабилизатором H. Заменяя пару (W, w)

на пару $(W \oplus W \otimes W, w + w \otimes w)$, можно считать, что орбита Gw пересекает прямую $\mathbb{K}w$ только в точке w. Для достаточно большого значения N в G-модуле $W \otimes V_2^{\otimes N}$ имеем

$$\lim_{t\to 0} \lambda(t)(w \otimes v_2^{\otimes N}) = 0$$

(отметим, что $\lambda(\mathbb{K}^*)$ можно рассматривать как подгруппу в G). С другой стороны, стабилизатор $w \otimes v_2^{\otimes N}$ совпадает с H. Следовательно, пространство G/H не является аффинно замкнутым.

Обратно, предположим что G/H допускает нетривиальное аффинное вложение. Этому вложению отвечает G-инвариантная подалгебра $A \subset \mathbb{K}[G/H]$, содержащая нетривиальный G-инвариантный идеал I. Заметим, что алгебру $\mathbb{K}[L]$ можно отождествить с подалгеброй в $\mathbb{K}[G]$, состоящей из (лево- или право-) G^u-инвариантных функций, $\mathbb{K}[G/H]$ реализуется в $\mathbb{K}[G]$ как подалгебра H-правоинвариантных функций, а $\mathbb{K}[L/K]$ — это G^u-левоинвариантные функции в $\mathbb{K}[G/H]$. Рассмотрим действие G^u на идеале I. Согласно теореме Ли—Колчина в I имеется ненулевой G^u-инвариантный элемент. Поэтому подалгебра $A \cap \mathbb{K}[L/K]$ содержит нетривиальный L-инвариантный идеал $I \cap \mathbb{K}[L/K]$. Таким образом, аффинная замкнутость пространства L/K противоречит следующей лемме.

Лемма 1. *Пусть L/K — аффинно замкнутое пространство редуктивной группы L. Тогда каждая L-инвариантная подалгебра в $\mathbb{K}[L/K]$ конечно порождена и не содержит нетривиальных L-инвариантных идеалов.*

Доказательство. Пусть $B \subset \mathbb{K}[L/K]$ — инвариантная подалгебра, которая не является конечно порожденной. Тогда для каждой цепочки $W_1 \subset W_2 \subset W_3 \subset \dots$ конечномерных L-инвариантных подмодулей в $\mathbb{K}[L/K]$, объединение которых совпадает с $\mathbb{K}[L/K]$, порожденные ими подалгебры $B_1 \subset B_2 \subset B_3 \subset \dots$ не совпадают с $\mathbb{K}[L/K]$ и не стабилизируются, поэтому можно считать, что все включения являются строгими. Пусть Z_i — аффинное L-многообразие, отвечающее алгебре B_i. Включение $B_i \subset \mathbb{K}[L/K]$ индуцирует доминантный морфизм $L/K \to Z_i$, и из теоремы 1 следует, что $Z_i = L/K_i$, $K \subset K_i$. Поскольку $B_1 \subset B_2 \subset B_3 \subset \dots$, каждая подгруппа K_i строго содержится в K_{i-1}, что невозможно. Итак, алгебра B конечно порождена и, как показано выше, группа L транзитивно действует на аффинном многообразии Z, отвечающем B, в то время как нетривиальный L-инвариантный идеал в B отвечает собственному L-инвариантному подмногообразию в Z. Теорема 2 доказана. □

Следствие 1. *Пусть однородное пространство G/H аффинно замкнуто. Тогда для произвольного аффинного G-многообразия и точки $x \in X$ такой, что $Hx = x$, орбита Gx замкнута.*

Доказательство. Из обозримости G_x в G следует обозримость $\phi(G_x)$ в L. Подгруппа $\phi(G_x)$ содержит $K = \phi(H)$ и по теореме 1 пространство $L/\phi(G_x)$ (а потому и G/G_x) аффинно замкнуто. □

Следствие 2. *Если X — аффинное G-многообразие и точка $x \in X$ неподвижна относительно некоторого максимального тора T группы G, то орбита Gx замкнута.*

3. G-алгебры с конечно порожденными инвариантными подалгебрами

Под *аффинной* алгеброй над полем $\mathbb{K}$ будем понимать конечно порожденную ассоциативную коммутативную $\mathbb{K}$-алгебру с единицей. Пусть F — подгруппа группы автоморфизмов аффинной алгебры $\mathscr{A}$ и $\operatorname{rad}(\mathscr{A})$ — совокупность нильпотентных элементов алгебры $\mathscr{A}$. Ясно, что $\operatorname{rad}(\mathscr{A})$ является F-инвариантным идеалов в $\mathscr{A}$.

Лемма 2. *Следующие условия эквивалентны*:

1) *каждая F-инвариантная подалгебра в $\mathscr{A}$ конечно порождена*;
2) *каждая F-инвариантная подалгебра в $\mathscr{A}/\operatorname{rad}(\mathscr{A})$ конечно порождена и* $\dim \operatorname{rad}(\mathscr{A}) < \infty$.

Доказательство. Каждое конечномерное подпространство в $\mathrm{rad}(\mathscr{A})$ порождает конечномерную подалгебру в $\mathscr{A}$, поэтому если $\mathrm{rad}(\mathscr{A})$ бесконечномерно, то порожденная этим подпространством подалгебра не является конечно порожденной. С другой стороны, прообраз в $\mathscr{A}$ не конечно порожденной подалгебры в $\mathscr{A}/\mathrm{rad}(\mathscr{A})$ не конечно порожден.

Обратно, пусть выполнено 2). Тогда каждая подалгебра в $\mathscr{A}$ порождается элементами, образы которых порождают образ этой подалгебры в $\mathscr{A}/\mathrm{rad}(\mathscr{A})$, и базисом пространства $\mathrm{rad}(\mathscr{A})$. □

Будем называть *G-алгеброй* аффинную алгебру $\mathscr{A}$ с заданным на ней действием (автоморфизмами) алгебраической группы G таким, что каждый элемент $a \in \mathscr{A}$ лежит в конечномерном G-инвариантном подпространстве, которое является (алгебраическим) G-модулем. Наша задача — описать все G-алгебры, для которых каждая G-инвариантная подалгебра конечно порождена. В силу леммы 2 мы можем далее предполагать что $\mathrm{rad}(\mathscr{A}) = 0$.

Пусть $X = \mathrm{Spec}(\mathscr{A})$ — аффинное многообразие, отвечающее аффинной алгебре $\mathscr{A}$ без нильпотентов. Задание на $\mathscr{A} = \mathbb{K}[X]$ структуры G-алгебры равносильно заданию на многообразии X (алгебраического) G-действия. Будем называть *размерностью* алгебры $\mathscr{A}$ размерность многообразия X.

Лемма 3. *Если размерность $\mathscr{A}$ не превосходит единицы, то каждая подалгебра в $\mathscr{A}$ конечно порождена.*

Доказательство. Случай, когда X неприводимо, разобран, например, в [5, Proposition 2]. Если $X = X_1 \cup \cdots \cup X_m$ — разложение на неприводимые компоненты, то $\mathscr{A}$ вкладывается в прямую сумму алгебр $\mathbb{K}[X_i]$, в каждой из которых любая подалгебра конечно порождена. Читатель легко завершит доказательство, рассмотрев проекцию $\mathscr{A}$ на $\mathbb{K}[X_1]$ и воспользовавшись индукцией по m. □

Лемма 4. *Пусть $X = Z_1 \cup Z_2$, где Z_1 и Z_2 — замкнутые инвариантные подмногообразия. Тогда следующие условия эквивалентны*:

1) *каждая инвариантная подалгебра в $\mathscr{A}$ конечно порождена*;
2) *каждая инвариантная подалгебра в $\mathbb{K}[Z_1]$ и в $\mathbb{K}[Z_2]$ конечно порождена.*

Доказательство. Если в $\mathbb{K}[Z_1]$ имеется не конечно порожденная инвариантная подалгебра, то достаточно рассмотреть ее прообраз при гомоморфизме ограничения $\mathbb{K}[X] \to \mathbb{K}[Z_1]$. Для доказательства обратного вложим $\mathbb{K}[X]$ в $\mathbb{K}[Z_1] \oplus \mathbb{K}[Z_2]$ и воспользуемся доказательством предыдущей леммы. □

Лемма 4 позволяет считать, что G транзитивно действует на множестве неприводимых компонент многообразия X.

Ниже мы обобщаем конструкцию из [5] на случай несвязных групп и приводимых многообразий. Пусть Y — замкнутое подмногообразие в X. Рассмотрим подалгебру

$$\mathscr{A}(X, Y) = \{f \in \mathbb{K}[X] \mid f(y_1) = f(y_2)\ \forall y_1, y_2 \in Y\}.$$

Лемма 5. *Если Y содержит неприводимую компоненту положительной размерности, не совпадающую ни с одной неприводимой компонентой X, то $\mathscr{A}(X, Y)$ не является конечно порожденной.*

Доказательство. Заметим, что $\mathscr{A}(X, Y) = \mathbb{K} \oplus I(Y)$. Если $\mathscr{A}(X, Y)$ конечно порождена, то можно считать, что образующие $f_1, \ldots, f_k$ лежат в $I(Y)$. Тогда моном степени s от $f_1, \ldots, f_k$ лежит в $I(Y)^s$. Поэтому достаточно доказать, что для некоторого l пространство $I(Y)/I(Y)^l$ бесконечномерно.

Пусть $Y = Y_1 \cup \cdots \cup Y_n$ и $X = X_1 \cup \cdots \cup X_m$ — разложение на неприводимые компоненты, причем $Y_1 \subset X_1$, $Y_1 \neq X_1$, $\dim Y_1 > 0$. Пусть $f \in I(Y)$ и $f \not\equiv 0$ на X_1. Пусть $\mathscr{O}_{X_1, Y_1}$ — локальное кольцо подмногообразия Y_1 в X_1 и $\mathscr{I}$ — его максимальный идеал. По лемме Накаямы $\bigcap\limits_{i=1}^{\infty} \mathscr{I}^i = 0$; поэтому

после ограничения на X_1 элемент f лежит в $\mathscr{I}^{l-1} \setminus \mathscr{I}^l$ для некоторого $l \geqslant 2$. Пусть W — подпространство в $\mathbb{K}[X]$, дополнительное к $I(Y_1)$. Заметим, что W бесконечномерно, так как $\dim Y_1 > 0$. Подпространство fW можно рассматривать как бесконечномерное подпространство в $\mathscr{I}^{l-1}$, тривиально пересекающееся с $\mathscr{I}^l$. Следовательно, fW определяет бесконечномерное подпространство в $I(Y)/I(Y)^l$.

Итак, каждое инвариантное подмногообразие Y, удовлетворяющее условиям леммы 5, определяет в $\mathbb{K}[X]$ не конечно порожденную инвариантную подалгебру $\mathscr{A}(X, Y)$. □

Пусть G^0 — связная компонента единицы группы G.

Теорема 3. *Пусть $\mathscr{A}$ — G-алгебра без нильпотентов с нетождественным действием подгруппы G^u. Следующие условия эквивалентны*:

1) *каждая G-инвариантная подалгебра в $\mathscr{A}$ конечно порождена*;
2) *каждая G-инвариантная подалгебра в $\mathscr{A}$ не содержит нетривиальных G-инвариантных идеалов*;
3) *каждая L-инвариантная подалгебра в $\mathscr{A}^{G^u}$ не содержит нетривиальных L-инвариантных идеалов*;
4) *$\mathscr{A} = \mathbb{K}[G/H]$ и пространство G/H аффинно замкнуто*;
5) *$\mathscr{A}^{G^u} = \mathbb{K}[L/K]$ и пространство L/K аффинно замкнуто.*

Доказательство. 1) $\Rightarrow$ 4) *Шаг 1.* Пусть действие $G : X$ нетранзитивно. Замыкание Y G-орбиты на X является инвариантным подмногообразием, к которому применима лемма 5, за исключением случаев $Y = X$ и $\dim Y = 0$. Следовательно, из 1) вытекает, что G^0 действует на каждой компоненте X_i с открытой орбитой, дополнение до которой есть конечный набор точек. В этой ситуации действие $G^u : X$ тождественно (см. [2, Theorem 3], [5, Proposition 4]).

Шаг 2. Пусть действие $G : X$ транзитивно. Тогда $X = G/H$. Предположим, что G/H допускает нетривиальное аффинное вложение $G/H \hookrightarrow X'$. Тогда $\mathbb{K}[X']$ — инвариантная подалгебра в $\mathscr{A}$ и, как показано на шаге 1, она содержит не конечно порожденную инвариантную подалгебру.

2) $\Rightarrow$ 4) Из отсутствия нетривиальных инвариантных идеалов в $\mathscr{A}$ следует, что $X = G/H$, а отсутствие инвариантных идеалов в подалгебрах гарантирует отсутствие у G/H нетривиальных вложений.

Доказательства импликаций 4) $\Rightarrow$ 1) и 4) $\Rightarrow$ 2) повторяют доказательство леммы 1 с использованием следствия 1. Аналогично доказывается импликация 5) $\Rightarrow$ 3).

Мы знаем, что $\mathbb{K}[G/H]^{G^u} = \mathbb{K}[L/K]$. Отсюда и из теоремы 2 следует импликация 4) $\Rightarrow$ 5).

3) $\Rightarrow$ 2) Пусть $\mathscr{B}$ — инвариантная подалгебра в $\mathscr{A}$ и I — нетривиальный инвариантный идеал в $\mathscr{B}$. Тогда $I \cap \mathscr{A}^{G^u}$ — нетривиальный инвариантный идеал в $\mathscr{B} \cap \mathscr{A}^{G^u}$. Теорема 3 доказана. □

Замечание. 1) Указанные в теореме 3 условия не эквивалентны условию «всякая L-инвариантная подалгебра в $\mathscr{A}^{G^u}$ конечно порождена»: достаточно рассмотреть $G = G^u = (\mathbb{K}, +)$, действующую на $\mathbb{K}[x, y]$ по формуле $(a, f(x, y)) \to f(x + ay, y)$.

2) Импликация 1) $\Rightarrow$ 5) неверна, если $\mathscr{A} = \mathscr{A}^{G^u}$ (см. [5]).

3) Ограничение $\mathscr{A} \neq \mathscr{A}^{G^u}$ оправдано тем, что случай действия редуктивной группы рассмотрен в [5]. Там предполагалось, что группа G связна и многообразие X неприводимо, однако из леммы 3 и сказанного выше следует, что если редуктивная группа G действует транзитивно на множестве компонент X, то каждая инвариантная подалгебра в $\mathbb{K}[X]$ конечно порождена в том и только том случае, когда либо G^0-алгебра $\mathbb{K}[X_i]$ имеет (в терминах [5]) тип C или HV, либо $X = G/H$ и G/H аффинно замкнуто (из последнего не следует, что G^0-алгебра $\mathbb{K}[X_i]$ имеет тип N; см. пример 5 в разделе 4). Интересно отметить, что предположение $\mathscr{A} \neq \mathscr{A}^{G^u}$ приводит к упрощению основных результатов.

Следствие 3. *Пусть G/H — квазиаффинное однородное пространство и H не содержит G^u. Тогда либо G/H аффинно замкнуто, либо имеется счетный набор попарно неизоморфных*

аффинных вложений $G/H \hookrightarrow X_i$ и последовательность доминантных эквивариантных морфизмов

$$X_1 \leftarrow X_2 \leftarrow X_3 \leftarrow \dots.$$

Доказательство. Пусть $G/H \hookrightarrow X$ — нетривиальное аффинное вложение и Y — дополнение до открытой орбиты в X. Как показано выше, алгебра $\mathscr{A}(X,Y)$ не конечно порождена. Пусть $g_0 \in I(Y)$ — ненулевой элемент и $f_1,\dots,f_s$ — система порождающих алгебры $\mathbb{K}[X]$. Положим $g_i = g_0 f_i$, $i = 1,\dots,s$, и дополним набор $g_0, g_1, \dots, g_s$ до (бесконечной) системы порождающих $g_0, g_1, \dots, g_s, h_1, h_2, \dots$ алгебры $\mathscr{A}(X,Y)$. Тогда аффинные G-многообразия X_i, отвечающие подалгебрам

$$\mathscr{B}_i = \mathbb{K}\left[\langle Gg_0, Gg_1, \dots, Gg_s, Gh_1, \dots, Gh_i\rangle\right] \subset \mathscr{A}(X,Y) \subset \mathbb{K}[X] \subset \mathbb{K}[G/H],$$

определяют вложения $G/H \hookrightarrow X_i$, и вложения подалгебр задают требуемую цепочку доминантных морфизмов. С другой стороны, в последовательности X_i можно выбрать бесконечную подпоследовательность, состоящую из попарно неизоморфных вложений. (По определению, изоморфизм двух вложений переводит отмеченную точку в отмеченную точку и является единственным морфизмом изоморфных вложений, действующим тождественно на открытой орбите.) □

4. Несколько замечаний об аффинных вложениях однородных пространств для нередуктивных групп

В этом разделе укажем несложные примеры, позволяющие отрицательно ответить на ряд естественных вопросов.

Пусть V — конечномерный G-модуль и $v \in V$.

Пример 1. Из замкнутости Gv не следует замкнутость Lv. Достаточно рассмотреть

$$V = \mathbb{K}^2, \quad v = (1,1), \quad G = \left\{\begin{pmatrix} t & a \\ 0 & 1 \end{pmatrix}\right\}, \quad L = \left\{\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}\right\}.$$

Пример 2. Из замкнутости Lv не следует замкнутость Gv. Здесь рассмотрим

$$V = \mathbb{K}^2, \quad v = (1,1), \quad G = \left\{\begin{pmatrix} t & a \\ 0 & t^{-1} \end{pmatrix}\right\}, \quad L = \left\{\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}\right\}.$$

Пример 3. Из того, что G/H аффинно замкнуто, не следует, что все L-орбиты на G/H замкнуты. Например, возьмем

$$G = \left\{\begin{pmatrix} t & a \\ 0 & t^{-1} \end{pmatrix}\right\}, \quad H = L = \left\{\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}\right\}, \quad x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \overline{LxH} \neq LxH.$$

Пример 4. Из аффинной замкнутости G^0/H^0 следует аффинная замкнутость G/H, однако обратное неверно. Можно рассмотреть ситуацию, где $G = SL(2)$, а H — произвольная неабелева конечная подгруппа.

Пример 5. Из аффинной замкнутости $G^0/(H \cap G^0)$ следует аффинная замкнутость G/H, однако обратное неверно. Рассмотрим

$$G = N_{SL(2)}T, \quad H = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Пример 6. Из того, что $0 \in \overline{Gv}$, не следует, что нуль реализуется как предел однопараметрической подгруппы в G. Соответствующий пример для разрешимой G приведен в [7, Sec. 11].

Открытой остается проблема характеризации аффинно замкнутых однородных пространств (как для редуктивной, так и для произвольной алгебраической группы) над алгебраически замкнутым полем положительной характеристики. В частности, не известно, имеет ли здесь место следствие 1. Некоторые результаты в этом направлении содержатся в [5, Sec. 8].

СПИСОК ЛИТЕРАТУРЫ

1. *Винберг Э. Б., Попов В. Л.* Теория инвариантов// Итоги науки и техн. Совр. пробл. мат. Фундам. напр. — М.: ВИНИТИ, 1989. — *55*. — С. 137–309.
2. *Попов В. Л.* Классификация трехмерных аффинных алгебраических многообразий, квазиоднородных относительно алгебраической группы// Изв. АН СССР. Сер. мат. — 1975. — *39*, № 3. — С. 566–609.
3. *Суханов А. А.* Описание наблюдаемых подгрупп линейных алгебраических групп// Мат. сб. — 1988. — *137*, № 1. — С. 90–102.
4. *Теннова Н. А.* Критерий аффинной замкнутости однородных пространств разрешимых групп// Вестн. МГУ (в печати).
5. *Arzhantsev I. V.* Algebras with finitely generated invariant subalgebras// Ann. Inst. Fourier. — 2003. — *53*, №. 2. — С. 379–398.
6. *Arzhantsev I. V., Timashev D. A.* Affine embeddings with a finite number of orbits// Trans. Groups. — 2001. — *6*, № 2. — С. 101–110.
7. *Birkes D.* Orbits of linear algebraic groups// Ann. Math. — 1971. — *93*, № 3. — С. 459–475.
8. *Gichev V. M., Latypov I. A.* Polynomially convex orbits of compact Lie groups// Trans. Groups. — 2001. — *6*, № 4. — С. 321–331.
9. *Grosshans F. D.* Algebraic homogeneous spaces and invariant theory/ Lect. Notes Math. — Berlin: Springer-Verlag, 1997. — *1673*.
10. *Latypov I. A.* Homogeneous spaces of compact connected Lie groups which admit nontrivial invariant algebras// J. Lie Theory. — 1999. — *9*. — С. 355–360.
11. *Luna D.* Adhérences d'orbite et invariants. — Invent. Math. — 1975. — *29*. — С. 231–238.

И. В. Аржанцев
Московский государственный университет им. М. В. Ломоносова
E-mail: arjantse@mccme.ru

Н. А. Теннова
Московский государственный университет им. М. В. Ломоносова
E-mail: tata@mccme.ru

Современная математика и ее приложения. Том 14 (2004). С. 128–136

УДК 512.76

О ПОЛУСТАБИЛЬНЫХ МОРИ РАССЛОЕНИЯХ НА КОНИКИ

© 2004 г. **Ю. Г. ПРОХОРОВ**

Аннотация. Изучены стягивания Мори—Фано с трехмерного многообразия на поверхность, удовлетворяющие условию полустабильности. Построено множество примеров.

СОДЕРЖАНИЕ

1. Введение

В настоящей работе предложен метод построения множества примеров стягиваний Мори трехмерного многообразия на поверхность (см. [1, 2, 8]). Мы отсылаем читателя к работам [4, 6] за терминологией теории минимальных моделей.

Пусть X — трехмерное нормальное комплексное пространство с лишь терминальными особенностями. Собственный сюръективный морфизм $f\colon X \to Z$ на нормальную аналитическую поверхность называется *Мори расслоением на коники*, если $f_*\mathscr{O}_X = \mathscr{O}_Z$ и антиканонический дивизор $-K_X$ является f-обильным. Мы интересуемся *локальной структурой* таких стягиваний и, таким образом, всегда будем предполагать, что Z и X — достаточно малые окрестности (или ростки) некоторой точки $o \in Z$ и слоя $f^{-1}(o)$ соответственно. Заметим, что мы не предполагаем, что X — алгебраическое многообразие и f — *экстремальное стягивание Мори* (т.е. X $\mathbb{Q}$-факториально и $\rho(X/Z) = 1$). В настоящей работе мы имеем дело с *полустабильными* Мори расслоениями на коники, которые появляются в полустабильной программе минимальных моделей (см. [9] и ссылки в этой работе).

Определение 1.1. Мори расслоение на коники $f\colon X \to Z \ni o$ называется *q-полустабильным*, если существует эффективный дивизор Картье $o \in T \subset Z$ такой, что пара (X, f^*T) дивизориально логтерминальна.

Ниже приведен «стандартный» пример такого стягивания.

Пример 1.2 (см. [1, Example 2.1])**.** Торическое стягивание

$$(\mathbb{P}^1 \times \mathbb{C}^2)/\boldsymbol{\mu}_n(0 : a; 1, -1) \to \mathbb{C}^2/\boldsymbol{\mu}_n(1, -1)$$

является q-полустабильным Мори расслоением на коники с $T = \{x_1x_2 = 0\}/\boldsymbol{\mu}_n$.

Ясно, что в определении 1.1 мы можем заменить T на общее гиперплоское сечение, проходящее через o. Мы покажем, что пример выше довольно специален: в большинстве случаев поверхность $f^{-1}(T)$ неприводима и нормальна.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 02-01-00441), грантов НШ-489.2003.1, НШ-1910.2003.1 и Отделения математики Российской Академии наук.

ISSN 1512–1712

Предложение 1.3. *Пусть $f\colon X \to Z \ni o$ — q-полустабильное Мори расслоение на коники и пусть T — общее гиперплоское сечение, проходящее через o.*

1) *Если T приводимо, то f аналитически изоморфно Мори расслоению на коники из примера* 1.2. *В частности, $Z \ni o$ — дювалевская точка типа A_{m-1}.*
2) *Если T неприводимо, то точка $Z \ni o$ неособа и пара (X, f^*T) чисто логтерминальна (plt). В этом случае $S := f^*T$ — нормальная поверхность с лишь циклическими факторособенностями типа* T *или дювалевскими типа A_n (определение* T*-особенностей см. в разделе* 2).

На практике довольно трудно построить нетривиальные примеры Мори расслоений на коники явно (ср. [1, §5]). Используя теорию деформаций, очень просто доказать существование (или несуществование) q-полустабильных Мори расслоений на коники (см. раздел 4). В частности, мы докажем следующую теорему.

Теорема 1.4. *Для любой трехмерной терминальной полустабильной особенности $U \ni P$ существует q-полустабильное Мори расслоение на коники $f\colon X \to Z \ni o$ с единственной особой точкой, которая аналитически изоморфна $U \ni P$.*

К сожалению, наши методы не отвечают на вопрос о существовании *алгебраических* Мори расслоений на коники.

Благодарности. Эта статья основывается на материале лекции, прочитанной в Киотском исследовательском институте математических наук 17 апреля 2003 г. Окончательная версия была подготовлена в университете г. Лилль в январе 2004 г. Я благодарен этим институтам за гостеприимство и поддержку.

2. Особенности класса T

Пусть группа $\boldsymbol{\mu}_n$ действует на $\mathbb{C}^2$ по правилу $(x, y) \to (\eta^a x, \eta^b y)$, где η — примитивный корень n-й степени из единицы и $\gcd(n, a) = \gcd(n, b) = 1$. В этом случае мы говорим, что фактор $\mathbb{C}^2/\boldsymbol{\mu}_n$ — особенность типа $\frac{1}{n}(a, b)$. Эта особенность может быть записана как $\frac{1}{n}(1, q)$ и, таким образом, с точностью до аналитического изоморфизма она определяется дробью n/q. Минимальное разрешение $\frac{1}{n}(1, q)$ может быть описано следующим образом.

Двойственный граф исключительных дивизоров является цепью гладких рациональных кривых, индексы самопересечения $-b_1, \dots, -b_\varrho$ которых определяются из следующей цепной дроби:

$$\frac{n}{q} = b_1 - \cfrac{1}{b_2 - \cfrac{1}{\dots \cfrac{1}{b_\varrho}}}. \tag{2.1}$$

Для краткости будем обозначать дробь в (2.1) через $[b_1, \dots, b_\varrho]$. Заметим, что представление циклической факторособенности в форме $\frac{1}{n}(1, q)$ не единственно: $\frac{1}{n}(1, q')$ определяет ту же самую особенность, если и только если $q \equiv q'$ или $qq' \equiv 1 \mod n$.

Определение 2.2. Говорят, что циклический факторособенность $\frac{1}{n}(a, b)$, не являющаяся дювалевской, имеет тип T (или является T-особенностью), если $(a + b)^2 \equiv 0 \mod n$. (Легко видеть, что это определение не зависит от представления в виде $\frac{1}{n}(a, b)$.)

Если $\frac{1}{n}(1, q)$ — T-особенность (соответственно, дювалевская особенность), то мы будем говорить, что n/q — T-дробь (соответственно, дювалевская дробь) и $[b_1, \dots, b_\varrho]$ — T-цепь (соответственно, дювалевская цепь). Таким образом, n/q является T-дробью, если и только если $\beta(n/q) \in \mathbb{Z}$.

Замечание 2.3. Если дробь n/q соответствует особенности индекса 2, то n/q является T-дробью автоматически. Легко видеть, что это влечет одно из двух равенств:

$$n/q = [4] \quad \text{или} \quad n/q = [3, 2, \dots, 2, 3]. \tag{2.4}$$

Более того, $\beta(n/q) = \varrho(n/q)$. Обратно, любая цепь, такая как в (2.4) имеет индекс 2.

Минимальные разрешения T-особенностей полностью описаны.

Предложение 2.5 (см. [5]). 1) *Если цепь* $[b_1, \dots, b_\varrho]$ *имеет тип* T, *то таковы же и цепи*

$$\text{(a)} \quad [2, b_1, \dots, b_\varrho + 1] \quad \textit{и} \quad \text{(b)} \quad [b_1 + 1, \dots, b_\varrho, 2]$$

2) *Каждая* T-*цепь может быть получена из одной из цепей* (2.4) *и применением шагов, описанных в* 1).

Теорема 2.6 (см. [7, Proposition 5.9], [5]). *Пусть* $S \ni P$ *— росток двумерной факторособенности. Следующие условия эквивалентны*:

1) $S \ni P$ *является дювалевской или имеет тип* T;
2) $S \ni P$ *имеет* $\mathbb{Q}$*-гореншейново одномерное сглаживающее пространство деформаций*;
3) *существует терминальная трехмерная особенность* $X \ni P$ *и вложение* $P \in S \subset X$ *такие, что* $S \subset X$ *является дивизором Картье в* P *и пара* (X, S) *чисто логтерминальна.*

3. Предварительные результаты

В этом разделе будет доказано предложение 1.3.

Пусть S — двумерное комплексное пространство, имеющее не хуже чем факторособенности, и пусть $\varphi\colon S \to T$ — стягивание на кривую. Предположим, что T — достаточно малая окрестность точки $o \in T$. Будем говорить, что φ *— лограсслоение на коники*, если дивизор $-K_S$ является φ-обильным. Если, кроме того, каждая особенность поверхности S имеет тип T или дювалевская, то мы будем говорить, что φ — T-*расслоение на коники*.

Лемма 3.1 (см. [8, Lemma 2.5]). *Пусть* $f\colon X \to Z \ni o$ *— Мори расслоение на коники и пусть* T *— эффективный дивизор* $\mathbb{Q}$*-Вейля на* Z *такой, что пара* (X, f^*T) *логканонична* (*соответственно, чисто логтерминальна*) *в некоторой точке* $P \in f^{-1}(o)$. *Тогда пара* (Z, T) *логканонична* (*соответственно, чисто логтерминальна*).

Лемма 3.2. *Пусть* $f\colon X \to Z \ni o$ *— q-полустабильное Мори расслоение на коники и пусть* T *— эффективный дивизор Картье такой, что пара* (X, f^*T) *дивизориально логтерминальна. Если* T *неприводим, то точка* $Z \ni o$ *неособа, и для общего гиперплоского сечения* $o \in T_{\mathrm{gen}} \subset Z$ *пара* (X, f^*T_{gen}) *чисто логтерминальна.*

Доказательство. Следует из леммы 3.1 и теоремы Бертини. □

Предложение 3.3. *Пусть* $f\colon X \to Z \ni o$ *— Мори расслоение на коники. Предположим, что существует эффективный дивизор Вейля* T *на* Z *такой, что пара* (X, f^*T) *логканонична. Если* T *приводим, то расслоение* f *аналитически изоморфно одному из следующих Мори расслоений на коники*:

1) f *— из примера* 1.2,
2) $X'/\boldsymbol{\mu}_2(1:0:0;1,1) \to \mathbb{C}^2/\boldsymbol{\mu}_2(1,1)$, *где* $X' = \{x_0^2 + x_1^2 + x_2^2\phi(u,v) = 0\} \subset \mathbb{P}^2_{x_0,x_1,x_2} \times \mathbb{C}^2_{u,v}$ *и* $\phi(u,v)$ *—* $\boldsymbol{\mu}_2$*-инвариант без кратных множителей* (см. [1, пример 2.3]).

В частности, точка $Z \ni o$ *— дювалевская типа* A_{m-1}.

Доказательство. Согласно лемме 3.1 T имеет в точности две компоненты T_1 и T_2. Рассмотрим замену базы

$$\begin{array}{ccc} X' & \xrightarrow{\upsilon} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Z' & \xrightarrow{\pi} & Z \end{array},$$

где Z' неособо, $Z = Z'/\boldsymbol{\mu}_n$, $X = X'/\boldsymbol{\mu}_n$ и $\boldsymbol{\mu}_n$ действует на Z' свободно в коразмерности один (см. [1, (1.9)]). Положим $S = f^*T$, $S' = \upsilon^{-1}(S)$, $T' = \pi^*(T)$, $T'_i = \pi^*(T_i)$ и $S'_i = f'^*T'_i$. Тогда пара (X', S') логканонична. Заменяя T'_1 и T'_2 на общие гиперплоские сечения, мы можем считать, что T'_1 неособо и пара $(S'_1, S'_1|_{S'_2})$ логканонична, где $S'_1|_{S'_2}$ — дивизор Картье на S'_1. В этой ситуации S'_1 имеет не хуже чем дювалевские особенности. Следовательно, многообразие X' горенштейново. Так как слой $f'^{-1}(o')$ приведен, то согласно [1, §2] на X/Z мы имеем только две возможности для действия $\boldsymbol{\mu}_n$. □

Начиная с этого места, мы будем рассматривать q-полустабильные Мори расслоения на коники $f\colon X \to Z \ni o$ такие, что пара (X, f^*T) является чисто логтерминальной (и размерность слоев не превосходит 1).

4. Построение q-полустабильных Мори расслоений на коники при помощи деформаций

Теорема 4.1. *Пусть $\varphi\colon S \to T \ni o_T$ — T-расслоение на коники. Существует q-полустабильное Мори расслоение на коники $f\colon X \to Z \ni o_Z$ с неособой базой и вложения*

$$\begin{array}{ccc} S & \hookrightarrow & X \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle f} \\ T & \xhookrightarrow{\upsilon} & Z \end{array}$$

такие, что $\upsilon(o_T) = o_Z$ и пара (X, S) чисто логтерминальна.

Построим X как одномерное семейство T-расслоений на коники.

Доказательство. Заменяя S и T на их компактификации, можем считать, что S и T проективны, $T \simeq \mathbb{P}^1$ и морфизм $\varphi\colon S \to T$ — гладкий вне $\varphi^{-1}(o_T)$. Пусть P_i — особые точки S.

Обозначим через $\mathrm{Def}(S)$ (соответственно, $\mathrm{Def}(S, P_i)$) базу пространства версальных деформаций S (соответственно, особенности $S \ni P_i$). Пусть $s\colon \mathcal{S} \to \mathrm{Def}(S)$ — версальное семейство. Таким образом, можно предполагать, что $S = s^{-1}(o)$ для некоторого $o \in \mathrm{Def}(S)$.

Из [3, Proposition 11.4] получаем существование следующей диаграммы морфизмов комплексных аналитических пространств:

$$\begin{array}{ccc} \mathcal{S} & \xrightarrow{\mathcal{F}} & \mathcal{T} = T \simeq \mathbb{P}^1 \\ \downarrow & & \downarrow \\ \mathrm{Def}\, S & \longrightarrow & \mathrm{Def}\, T = \mathrm{pt} \end{array},$$

где $\mathcal{F}(S) = T$ и $\mathcal{F}|_S = \varphi$.

Имеется естественный морфизм (прообраз) ростков аналитических пространств

$$\mathrm{Def}\, S \longrightarrow \prod_i \mathrm{Def}(S, P_i). \tag{4.2}$$

Препятствия к глобализации деформаций в $\prod_i \mathrm{Def}(S, P_i)$ лежат в $R^2\varphi_*\Theta_S$, где $\Theta_S = (\Omega^1_S)^\vee$ — касательный пучок к S. Так как $R^2\varphi_*\Theta_S = 0$, то морфизм (4.2) является гладким. В частности, каждая деформация особенностей $S \ni P_i$ может быть глобализована (ср. [3, 11.4.2]).

Согласно теореме 2.6 каждая особенность S допускает $\mathbb{Q}$-гоpенштейново одномерное сглаживание. Следовательно, существует сглаживание $g\colon X \to \Delta \ni 0$, где $g^{-1}(0) = S$, X является $\mathbb{Q}$-гоpенштейновым и $\Delta \subset \mathbb{C}$ — малый диск. По обращению присоединения пара (X, S) чисто логтерминальна и, поскольку S — дивизор Картье, то X имеет не хуже чем терминальные особенности вблизи S.

Положим $Z = T \times \Delta$ и пусть $f\colon X \to Z$ — проекция. Ясно, что $f|_S = \varphi\colon S \to T$. Следовательно, дивизор $-K_X$ является f-обильным вблизи S. Уменьшая Z, мы получим Мори расслоение на коники $f\colon X \to Z \ni o = (o_T, 0)$. □

5. Примеры

В этом разделе будут построены примеры Т-расслоений на коники. Тот же самый подход был использован в [2] в доказательстве существования 1-дополнений.

Обозначения 5.1. Пусть $\varphi\colon S \to T \ni o$ — лограсслоение на коники. Предположим, что S имеет по крайней мере одну недювалевскую особенность. Пусть $\mu\colon \tilde{S} \to S$ — минимальное разрешение и $\phi\colon \tilde{S} \to T$ — композиция. Возьмем эффективный дивизор Картье D на S такой, что $\operatorname{Supp}(D) = \varphi^{-1}(o)$ и $-D$ является φ-численно эффективным. Например, можем положить $D = \varphi^*(o)$ (схемный слой).

Можно записать стандартную формулу

$$\mu^* K_S = K_{\tilde{S}} + \Delta, \tag{5.2}$$

где Δ — эффективный исключительный дивизор, так называемый *дивизор кодискрепантностей*. Так как особенности S логтерминальны, то $\lceil \Delta \rceil = 0$. Запишем также $\mu^* D = \sum l_i L_i + e_j E_j$, где E_i (соответственно L_i) — μ-исключительные (соответственно не-μ-исключительные) компоненты и $l_i, e_i \in \mathbb{N}$. Положим $L = \sum l_i L_i$ и $E = e_j E_j$. Таким образом, $D = \mu_* L$ и $\operatorname{Supp}(\Delta) \subset \sum E_i$.

Лемма 5.3. *В обозначениях выше имеем*:

(i) $\operatorname{Supp}(L + E)$ — *дерево гладких рациональных кривых*;
(ii) *все компоненты* L *являются* (-1)-*кривыми*;
(iii) $\Delta \cdot L_i < 1$ *для всех* i;
(iv) $L \cdot \Delta + 2 = \sum l_i$.

Доказательство. Доказательства утверждений (i)–(iii) см. в [2, лемма 4.3]. Для доказательства (iv) заметим, что $\mu^* K_S \cdot L = -2$. Таким образом,

$$\sum l_i = -K_{\tilde{S}} \cdot L = -\mu^* K_S \cdot L + \Delta \cdot L = \Delta \cdot L + 2.$$

Лемма доказана. □

Замечание 5.4. 1) Легко видеть, что условие (iii) леммы 5.3 является также достаточным. Предположим, что условия 5.1 имеют, место за исключением обильности $-K_S$. Если $\Delta \cdot L_i < 1$ для всех i, то φ — лограсслоение на коники, т.е. дивизор $-K_S$ обилен.

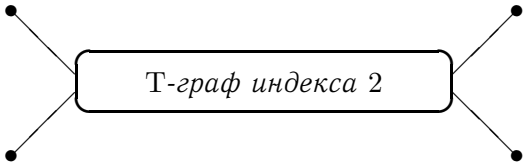
2) Если S имеет единственную недювалевскую точку, то условие (iii) леммы 5.3 выполняется автоматически.

Для того чтобы описывать лограсслоения на коники, введем язык взвешенных графов. Под *взвешенным* графом Γ понимаем граф, каждой вершине которого поставлен в соответствие вес $b_i \geqslant 1$. С каждым взвешенным графом $\Gamma = \{v_1, \ldots, v_\varrho\}$ ассоциируем квадратичную форму, полагая $v_i^2 = -b_i$, причем $v_i \cdot v_j$ при $i \neq j$ равно числу ребер, соединяющих v_i и v_j. Будем говорить, что взвешенный граф $\Gamma = \{v_1, \ldots, v_\varrho\}$ является *параболическим*, если ассоциированная квадратичная форма имеет сигнатуру $(0, \varrho - 1)$. Вершины с $b_i = 1$ будут называться (и изображаться) *черными*, а вершины с $b_i \geqslant 2$ — *белыми*. Веса $b_i = 1$ и $b_i = 2$ будем опускать.

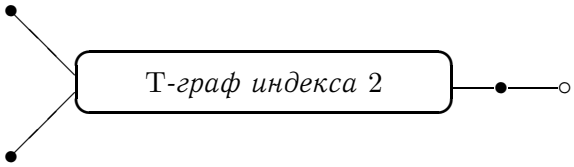
Теперь, используя 5.1, обозначим через $\Gamma(\varphi)$ двойственный граф слоя $\phi^{-1}(o)$. Согласно п. (i) леммы 5.3 граф $\Gamma(\varphi)$ является деревом. Более того, граф $\Gamma(\varphi)$ является параболическим.

Предложение 5.5. *Пусть* $\varphi\colon S \to T$ *— двумерное лограсслоение на коники индекса* 2. *Тогда граф* $\Gamma(\varphi)$ *– один из следующих*:

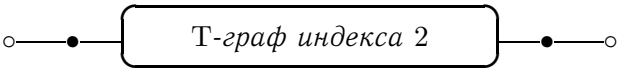
(I*)



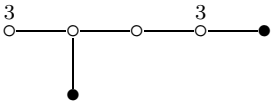
(I**)



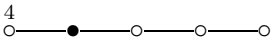
(I***)



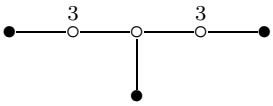
(II*)



(III*)



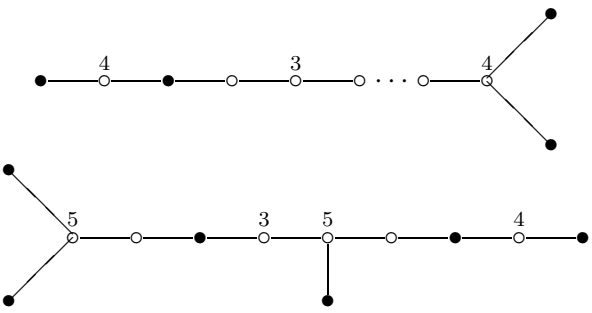
(III**)



Обозначения (I*)–(III**) могут быть объяснены следующим образом. Рассмотрим общий элемент $B \in |-K_S|$ и пусть $S' \to S$ — двойное накрытие разветвленное в B. Тогда $K_{S'} = 0$, $S' \to T$ — эллиптическое расслоение и S' имеет только дювалевские особенности (ср. [1, §3]). Если $\tilde{S}'$ — минимальное разрешение, то центральный слой композиции $\tilde{S}' \to T$ — особый слой Кодаиры.

Доказательство. Для любой логтерминальной точки индекса 2 все логдискрепантности минимального разрешения равны $1/2$. Согласно лемме 5.3 существует не более одной недювалевской точки на каждой компоненте D. Согласно [2, следствие 4.5] существует в точности одна недювалевская точке P на S, и все компоненты D проходят через P. Снова используя лемму 5.3, получаем $\sum l_i = 4$. Таким образом, граф $\Gamma(\varphi)$ имеет не более четырех черных вершин. Теперь классификация вытекает из [2, лемма 4.4]. □

Пример 5.6. Следующие графы дают примеры T-расслоений на коники с двумя и тремя недювалевскими точками:



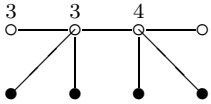
Предложение 5.7. *Для любой* T*-особенности* $\frac{1}{n}(1,q)$ *существует* T*-расслоение на коники с ровно одной особой точкой, которая имеет тип* $\frac{1}{n}(1,q)$.

Доказательство. Можем начать с графа (I*) и применить конструкцию 5.8 (см. ниже). Согласно предложению 2.5 на каждом шаге будем иметь только особенности типа T. □

Конструкция 5.8. Под *раздутием вершины* v_i взвешенного графа Γ понимаем следующее преобразование: вес вершины v_i уменьшается на 1, т.е. $b'_i = b_i + 1$, и к графу добавляется новая черная вершина, связанная ребром с v'_i. Нетрудно видеть, как это преобразование соотносится с раздутиями на неособой поверхности.

Пусть φ — лограсслоение на коники с единственной особой точкой типа $[b_1, \dots, b_\varrho]$. Предположим, что в $\Gamma(\varphi)$ существует черная вершина, соединенная с концом b_1, т.е. $\Gamma(\varphi)$ содержит цепь $[1, b_1, \dots, b_\varrho]$, где $[b_1, \dots, b_\varrho]$ соответствует особой точке. Раздувая концы 1 и b_ϱ, получим граф Γ', содержащий цепь $[1, 2, b_1, \dots, b_\varrho + 1, 2]$. Согласно замечанию 5.4 Γ' соответствует лограсслоению на коники (т.е. антиканонический дивизор обилен).

Замечание 5.9. 1) Конструкция 5.8 дает только одну серию T-расслоений на коники с единственной особой точкой. Например, следующее T-расслоение на коники не может быть получено этим способом:



2) Аналогично конструкции 5.8 можно получить бесконечные серии T-расслоений на коники с двумя и тремя особыми точками, начиная с примера 5.6.

6. Случай неприводимого центрального слоя

Следующая лемма показывает, что случай, когда относительное число Пикара равно 1, наиболее важен. Напомним, что собственный сюръективный морфизм $f\colon X \to Z$ с трехмерного нормального комплексного пространства с лишь терминальными особенностями называется *стягиванием Фано—Мори*, если $f_*\mathscr{O}_X = \mathscr{O}_Z$ и антиканонический дивизор $-K_X$ является f-обильным.

Лемма 6.1. *Пусть* $f\colon X \to Z \ni o$ *— стягивание Фано—Мори такое, что размерность слоев не превосходит* 1. *Существует стягивание Фано—Мори* $f'\colon X' \to Z$ *с тем же свойством и бирациональное отображение* $h\colon X \dashrightarrow X'$ *над* Z *такие, что* h *является морфизмом вне* $f^{-1}(o)$, X' $\mathbb{Q}$*-факториально и* $\rho(X/Z) = 1$. *В частности, прообраз* $f'^{-1}(L)$ *неприводим для любого неприводимого дивизора* $L \subset Z$. *Если, кроме того, пара* (X, f^*T) *дивизориально логтерминальна для некоторого эффективного дивизора Картье* T, *то можно взять* X' *так, что пара* $(X', f'^*(T))$ *дивизориально логтерминальна.*

Доказательство. Пусть $q\colon X^{\mathrm{q}} \to X$ — $\mathbb{Q}$-факториальная модификация. Тогда X^{q} имеет только терминальные $\mathbb{Q}$-факториальные особенности, $K_{X^{\mathrm{q}}} = q^*K_X$ и q — малое бирациональное стягивание. Применим программу минимальных моделей (ПММ) над Z. Получим X', как требовалось выше.

Для того чтобы доказать второе утверждение, рассмотрим $\mathbb{Q}$-факторизацию $q\colon X^{\mathrm{q}} \to X$ пары (X, S). Тогда пара $(X^{\mathrm{q}}, S^{\mathrm{q}})$ дивизориально логтерминальна, где $S^{\mathrm{q}} = q^*S$. Теперь осталось заметить, что $K_{X^{\mathrm{q}}}$-ПММ является в то же время и $K_{X^{\mathrm{q}}} + S^{\mathrm{q}}$-ПММ. □

Так как мы работаем в аналитической ситуации, то условие $\rho(X/Z) = 1$ влечет неприводимость слоя $f^{-1}(o)$. Далее мы классифицируем q-полустабильные Мори расслоения на коники с неприводимым центральным слоем.

Предложение 6.2 (ср. [8, Theorem 2.5]). *Пусть $\varphi\colon S \to T \ni o$ — T-расслоение на коники, имеющее по крайней мере одну недювалевскую точку. Предположим, что слой $D = \varphi^*(o)$ неприводим. Тогда φ имеет тип* (III*) *из предложения* 5.5.

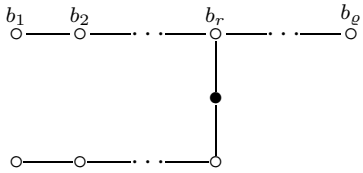
Следствие 6.3. *Пусть $f\colon X \to Z \ni o$ — q-полустабильное Мори расслоение на коники такое, что $f^{-1}(o)$ неприводим. Тогда X имеет ровно одну негорештейнову точку и эта точка имеет индекс* 2 (см. [1, §3]).

Доказательство. Если дивизор $K_S + C$ чисто логтерминален, то S имеет две особенности типов $\frac{1}{n}(1, q)$ и $\frac{1}{n}(1, n-q)$ (см. [8, Theorem 2.5]). Если обе они типа T, то

$$(q+1)^2 \equiv 0 \mod n, \quad (n-q+1)^2 \equiv 0 \mod n.$$

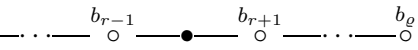
Это дает $4 \equiv 0 \mod n$. Так как особенности S хуже чем дювалевские, то $n = 4$. Получим случай (III*).

Теперь рассмотрим случай, когда дивизор $K_S + C$ не является чисто логтерминальным. Согласно [2, лемма 4.6, следствие 4.5] поверхность S имеет ровно одну недювалевскую точку и не более одной недювалевской точки Q. Более того, $S \ni Q$ имеет тип A_n и дивизор $K_S + C$ чисто логтерминален вблизи Q. Таким образом, $\Gamma(\varphi)$ имеет следующий вид:



(6.4)

где $r \neq 1$, $r \neq \varrho$. Стягивая последовательно черные вершины, на некотором шаге получим подграф



(6.5)

Лемма 6.6. *Если граф* (6.5) *является параболическим, то*

$$\sum_{i=1}^{r-1}(b_i - 1) = \sum_{j=r+1}^{\varrho}(b_j - 1) = \varrho - 2. \tag{6.7}$$

В частности, $r \neq 1, \varrho$.

Применим конструкцию, описанную в предложении 2.5, к $[b_1, \ldots, b_r, \ldots, b_\varrho]$. Каждый шаг сохраняет соотношение (6.7). В конце получим цепь $[b'_1, \ldots, b'_{r'}, \ldots, b'_{\varrho'}]$ такую, как в (2.4). Соотношение (6.7) дает $r' = \varrho' - r' + 1 = \varrho' - 2$, т.е. $r' = 3$ и $\varrho' = 5$. Следовательно, в (6.5) имеем $b_{r-1} = b_{r+2} = 2$. Это противоречит [2, лемма 4.4]. □

СПИСОК ЛИТЕРАТУРЫ

1. *Прохоров Ю. Г.* О дополняемости канонического дивизора для Мори расслоений на коники// Мат. сб. — 1997. — *188*, № 11. — С. 99–120.
2. *Прохоров Ю. Г.* О полустабильных стягиваниях Мори// Изв. РАН. Сер. мат. — 2004. — *68*, № 2.
3. *Kollár J., Mori S.* Classification of three-dimensional flips// J. Amer. Math. Soc. — 1992. — *5*. — С. 533–703.
4. *Kollár J., Mori S.* Birational geometry of algebraic varieties/ Cambridge Tracts Math. — Cambridge: Cambridge Univ. Press, 1998. — *134*.
5. *Kollár J., Shepherd-Barron N. I.* Threefolds and deformations of surface singularities// Invent. Math. — 1988. — *91*. — С. 299–338.
6. *Kollár J. et al.* Flips and abundance for algebraic threefolds// Astérisque. — 1992. — *211*.

7. *Looijenga E., Wahl J.* Quadratic functions and smoothing surface singularities// Topology. — 1986. — *25*. — С. 261–291.
8. *Prokhorov Yu. G.* Mori conic bundles with a reduced log terminal boundary// J. Math. Sci. — 1999. — *94*. — С. 1051–1059.
9. *Shokurov V. V.* Semistable 3-fold flips// Изв. РАН. Сер. мат. — 1993. — *57*, № 2. — С. 165–224.

Ю. Г. Прохоров
Московский государственный университет им. М. В. Ломоносова
E-mail: prokhoro@mech.math.msu.su

Современная математика и ее приложения. Том 14 (2004). С. 137–141

О ВЛОЖЕНИЯХ НЕКОТОРЫХ ФАКТОРАЛГЕБР СВОБОДНОЙ СУММЫ АЛГЕБР ЛИ

© 2004 г. **А. Л. ШМЕЛЬКИН, А. В. СЫРЦОВ**

Пусть Λ — коммутативное кольцо с единицей; $(B_i)_{i\in I}$ — некоторое семейство Λ-алгебр Ли; X — свободная Λ-алгебра Ли с базой $\{x_j \mid j \in J\}$; $F = (\sum_{i\in I}^{*} B_i) * X$ — их свободная сумма; R — такой идеал алгебры F, что $R \cap B_i = 1$, $i \in I$; V — такое многообразие Λ-алгебр Ли, что $\mathbf{V}(R)$ — идеал алгебры F. Построим при некоторых ограничениях вложение факторалгебры $F/\mathbf{V}(R)$ в вербальное V-сплетение свободной алгебры многообразия V и F/R и изучим это вложение. Отметим, что основные результаты данной работы являются обобщениями результатов А. Л. Шмелькина [4] и аналогом для алгебр Ли групповых результатов, полученных Н. С. Романовским [2].

Напомним определение вербального V-сплетения алгебр Ли (см. также [3]). Если A — алгебра Ли, принадлежащая многообразию V, B — произвольная алгебра Ли, то их вербальное V-сплетение $W = A \operatorname{wr}_V B$ определяется следующими свойствами:

1) W порождается подалгебрами A и B;
2) идеал, порожденный в W подалгеброй A, принадлежит многообразию V;
3) W универсальна относительно свойств 1) и 2), т.е. если имеются гомоморфизмы $\varphi : A \to L$, $\psi : B \to L$ в какую-либо алгебру L такие, что идеал, порожденный $\varphi(A)$ в L, принадлежит многообразию V, то существует гомоморфизм $W \to L$, продолжающий φ и ψ.

Напомним, что если $x_1, \ldots, x_{n-1}, x_n$ — элементы алгебры Ли L, то их левонормированный коммутатор $x_1 \ldots x_{n-1} x_n$ определяется индуктивно следующим образом:

$$x_1 \ldots x_{n-1} x_n = [(x_1 \ldots x_{n-1}), x_n], \quad n \geqslant 2.$$

Отождествим алгебры Ли B_i, $i \in I$, с их естественными образами в F/R и в $F/\mathbf{V}(R)$. Обозначим через $\bar{x}$ (через $\hat{x}$) естественный образ в F/R (в $F/\mathbf{V}(R)$) элемента $x \in X$.

Пусть $B = F/R$. Будем считать выполненными следующие два условия:

1) B — свободный Λ-модуль,
2) для любого i, B_i — свободный Λ-модуль, и любой его базис может быть дополненным до базиса B.

Из первой части условия 2) следует, что F — свободный Λ-модуль.

В дальнейшем, пусть A — свободная алгебра многообразия V со свободным порождающим множеством $\{a_k \mid k \in I \cup J\}$, $W = A \operatorname{wr}_V B$ — вербальное V-сплетение A и B, T — идеал, порожденный алгеброй A в W. Идеал T является свободной алгеброй многообразия V с базой, состоящей из всех левонормированных коммутаторов вида

$$a_k e_1 \cdots e_r, \quad e_1 \leqslant \cdots \leqslant e_r, \quad e_i \in E, \quad r \geqslant 0, \quad k \in I \cup J,$$

E — некоторый вполне упорядоченный базис алгебры B.

Рассмотрим сначала случай, когда V — многообразие абелевых алгебр Ли. В этом случае T — свободный $U(B)$-модуль, где $U(B)$ — универсальная обертывающая алгебры B. Из этого нетрудно вывести следующую лемму.

Лемма 1. *Пусть $\{E_k \mid k \in I \cup J\}$ — набор вполне упорядоченных базисов свободного модуля B. Тогда множество левонормированных коммутаторов вида*

$$a_k e_{k1} \ldots e_{kr}, \quad e_{k1} \leqslant \ldots \leqslant e_{kr}, \quad e_{ks} \in E_k, \quad k \in I \cup J, \quad r \geqslant 0,$$

образует базис T.

ISSN 1512–1712

Доказательство. Так как идеал T абелев, то для любого $t \in T$ определен внутренний автоморфизм $\exp(\operatorname{ad} t)$ алгебры W:

$$(\exp(\operatorname{ad} t))(x) = x + [t, x],$$

где $x \in W$. Таким образом, отображения

$$B_i \to (\exp(\operatorname{ad} a_i))(B_i), \quad i \in I,$$

определенные по следующему правилу:

$$\text{если } b_i \in B_i, \text{ то } b_i \to (\exp(\operatorname{ad} a_i))(b_i) = b_i + r_{b_i},$$

где $r_{b_i} = [a_i, b_i]$, являются мономорфизмами $B_i \to W$. Эти мономорфизмы, а также гомоморфизм

$$X \to W : x_j \to \bar{x}_j + a_j, \quad j \in J,$$

порождают гомоморфизм $\varphi : F \to W$, который, в свою очередь, индуцирует гомоморфизм $\hat{\varphi} : F/R^2 \to W$. □

Теорема 1. *Гомоморфизм $\hat{\varphi}$ является мономорфизмом.*

Доказательство. Рассмотрим вложение ξ алгебры F/R^2 в некоторое полупрямое произведение $B \leftthreetimes S$, обладающее следующими свойствами:

$$\xi(b_i) = b_i + s_{b_i}, \quad s_{b_i} \in S, \quad b_i \in B_i, \quad i \in I; \qquad \xi(\hat{x}_j) = \bar{x}_j + s_j, \quad s_j \in S, \quad j \in J;$$

такое вложение существует (см. [3]). Поскольку

$$\xi([b_i, b_i']) = [b_i, b_i'] + s_{[b_i, b_i']},$$
$$\xi([b_i, b_i']) = [b_i, b_i'] + [b_i, s_{b_i'}] + [s_{b_i}, b_i'],$$

имеет место формула

$$s_{[b_i, b_i']} = [b_i, s_{b_i'}] + [s_{b_i}, b_i']. \tag{1}$$

Также справедлива формула дистрибутивности:

$$s_{\alpha b_i + \beta b_i'} = \alpha s_{b_i} + \beta s_{b_i'}. \tag{1'}$$

Аналогично, имеют место формулы:

$$r_{[b_i, b_i']} = [b_i, r_{b_i'}] + [r_{b_i}, b_i'], \tag{2}$$
$$r_{\alpha b_i + \beta b_i'} = \alpha r_{b_i} + \beta r_{b_i'}, \quad r_{b_i} = [a_i, b_i]. \tag{2'}$$

Покажем, что существует гомоморфизм ψ из образа $\hat{\varphi}$ на образ ξ со следующим свойством:

$$\psi(b_i + r_{b_i}) = b_i + s_{b_i}, \quad \psi(\bar{x}_j + a_j) = \bar{x}_j + s_j,$$

т.е. $\psi\hat{\varphi} = \xi$. Достаточно доказать, что любое соотношение, выполненное на некоторых элементах множества

$$M_1 = \{b_i + r_{b_i} \mid b_i \in B_i,\ i \in I\} \sqcup \{\bar{x}_j + a_j \mid j \in J\},$$

выполнено также и на соответствующих элементах множества

$$M_2 = \{b_i + s_{b_i} \mid b_i \in B_i,\ i \in I\} \sqcup \{\bar{x}_j + s_j \mid j \in J\}.$$

Пусть $m(z_1, \ldots, z_n)$ — такой лиевский многочлен, что $m(m_{11}, \ldots, m_{1n}) = 0$, где $m_{1k} \in M_1$. Покажем, что $m(m_{21}, \ldots, m_{2n}) = 0$, где $m_{2k} \in M_2$; $m_{2k} = b_i + s_{b_i}$, если $m_{1k} = b_i + r_{b_i}$, $i \in I$; $m_{2k} = \bar{x}_j + s_j$, если $m_{1k} = \bar{x}_j + a_j$, $j \in J$. Для каждого i выберем базис E_i, $E_i = \{e_{ik} \mid k \in K_i\}$, алгебры B, включающий в себя базис алгебры B_i. Упорядочим полученный базис, считая элементы из B_i меньшими остальных элементов выбранного базиса. Зафиксируем также еще один упорядоченный базис E алгебры B, $E = \{e_k \mid k \in K\}$.

Из леммы следует, что множество Q, состоящее из левонормированных коммутаторов вида

$$r_{e_{i1}} e_{i2} \ldots e_{in}, \quad r_{e_{i1}} = [a_i, e_{i1}], \quad e_{i1} \leqslant \ldots \leqslant e_{in}, \quad e_{ik} \in E_i, \quad i \in I, \quad n \geqslant 0;$$
$$a_j e_1 \ldots e_n, \quad e_1 \leqslant \ldots \leqslant e_n, \quad e_k \in E, \quad n \geqslant 0, \quad j \in J,$$

— линейно независимое множество. Пользуясь тождествами антикоммутативности, Якоби, дистрибутивности, формулами (2) и (2′), законом умножения в B, приведем выражение $m(m_{11},\dots,m_{1n})$ к сумме двух элементов, первый из которых, p, принадлежит B, второй, Σ_1, представляет собой линейную комбинацию элементов Q. Так как $m(m_{11},\dots,m_{1n})=0$, $p\in B$, $\Sigma_1\in T$, $B\cap T=0$, то $\Sigma_1=0$ и $p=0$. Если в выражении Σ_1 заменить $r_{e_{i1}}$ на $s_{e_{i1}}$ и a_j на s_j, то, поскольку (1), (1′) вполне подобны (2), (2′), то полученное выражение Σ_2 будет равно $m(m_{21},\dots,m_{2n})$. Согласно лемме 1 все коэффициенты в выражении Σ_1 равны нулю. Значит, $\Sigma_2=0$. Мы показали, что существует гомоморфизм ψ из образа $\hat\varphi$ на образ ξ со свойством $\psi\hat\varphi=\xi$. Так как ξ — вложение, то $\hat\varphi$ — мономорфизм. Теорема доказана. □

Пусть N — ассоциативная алгебра матриц вида

$$\begin{pmatrix} u & 0\\ t & 0\end{pmatrix},\quad u\in U(B),\quad t\in T.$$

Множество M матриц вида

$$\begin{pmatrix} b & 0\\ t & 0\end{pmatrix},\quad b\in B,\quad t\in T,$$

образует подалгебру Ли в $N^{(-)}$. Естественным образом отождествим сплетение W с алгеброй Ли M. Приведем критерий принадлежности элемента сплетения W образу $\hat\varphi$.

Теорема 2. *Матрица*

$$\begin{pmatrix} u & 0\\ \sum\limits_{i\in I}a_iu_i+\sum\limits_{j\in J}a_ju_j & 0\end{pmatrix}$$

тогда и только тогда принадлежит образу $\hat\varphi$, когда

1) *при любом i, u_i лежит в правом идеале, порожденном B_i в $U(B)$,*
2) *в $U(B)$ справедливо равенство*

$$\sum_{i\in I}u_i+\sum_{j\in J}\bar x_ju_j=u.$$

Доказательство. Непосредственно проверяется, что условия 1), 2) выделяют в W подалгебру. Так как порождающие элементы

$$\begin{pmatrix} b_i & 0\\ a_ib_i & 0\end{pmatrix},\quad b_i\in B_i,\quad i\in I,\qquad \begin{pmatrix} \bar x_j & 0\\ a_j & 0\end{pmatrix},\quad j\in J,$$

алгебры $\hat\varphi(F/R^2)$ удовлетворяют этим условиям, то им также удовлетворяют все элементы из $\hat\varphi(F/R^2)$. Необходимо доказать обратное: элемент из W, удовлетворяющий условиям 1), 2), принадлежит $\hat\varphi(F/R^2)$. Пусть матрица

$$c=\begin{pmatrix} u & 0\\ \sum\limits_{i\in I}a_iu_i+\sum\limits_{j\in J}a_ju_j & 0\end{pmatrix}$$

удовлетворяет условиям 1), 2). В алгебре F/R^2 существует элемент g такой, что

$$\hat\varphi(g)=\begin{pmatrix} u & 0\\ * & 0\end{pmatrix}.$$

Заменим c на $(c-\hat\varphi(g))$. Эта замена сводит задачу к случаю, когда c является нижнетреугольной матрицей с нулевой диагональю и имеет место соотношение

$$\sum_{i\in I}u_i+\sum_{j\in J}\bar x_ju_j=0.$$

Гомоморфизм φ порождает гомоморфизм ассоциативных алгебр $\alpha : U(F) \to N$. Обозначим через β естественный гомоморфизм $U(F) \to U(B)$. Очевидно,

$$\alpha(h) = \begin{pmatrix} \beta(h) & 0 \\ * & 0 \end{pmatrix}, \quad h \in U(F).$$

Для элемента u_i, $i \in I$, выберем в кольце $U(F)$ прообраз v_i, принадлежащий $U(F)B_i$, т.е. $\beta(v_i) = u_i$. Для u_j, $j \in J$, выберем произвольный прообраз v_j, т.е. $\beta(v_j) = u_j$.

Пусть

$$v = \sum_{i \in I} v_i + \sum_{j \in J} x_j v_j.$$

Прямое вычисление показывает, что $\alpha(v) = c$. Поэтому $v \in \ker \beta$. Следовательно, v можно представить в виде

$$v = \sum_{s=1}^{m} r_s f_{s1} \cdots f_{sn_s},$$

где $f_{kl} \in F$, $n_s \geqslant 0$, $r_s \in R$.

Пусть

$$f = \sum_{s=1}^{m} \overline{r_s f_{s1} \cdots f_{sn_s}},$$

где $\overline{r_s f_{s1} \cdots f_{sn_s}}$ — левонормированные коммутаторы, соответствующие ассоциативным произведениям $r_s f_{s1} \cdots f_{sn_s}$. Тогда $f \in R$. Непосредственно проверяется, что $\alpha(f) = \alpha(v) = c$. Значит, $\hat{\varphi}(f + R^2) = c$. □

Рассмотрим теперь случай, когда Λ — поле характеристики 0, V — нильпотентное многообразие. Так как идеал T нильпотентен, то для любого $t \in T$ определен внутренний автоморфизм

$$\exp(\operatorname{ad} t) = \sum_{k=0}^{+\infty} \frac{(\operatorname{ad} t)^k}{k!}.$$

Таким образом, отображения $B_i \to (\exp(\operatorname{ad} a_i)(B_i)$ являются мономорфизмами $B_i \to W$. Эти мономорфизмы, а также гомоморфизм $X \to W : x_j \to \bar{x}_j + a_j$ порождают гомоморфизм $\varphi : F \to W$, который, в свою очередь, индуцирует гомоморфизм $\tilde{\varphi} : F/\mathbf{V}(R) \to W$.

Теорема 3. *Гомоморфизм $\tilde{\varphi}$ является мономорфизмом.*

Доказательство. Достаточно показать, что ограничение $\tilde{\varphi}$ на $R/\mathbf{V}(R)$ является мономорфизмом. В [1] доказано, что R — свободная алгебра Ли. Следовательно, $R/\mathbf{V}(R)$ — свободная алгебра Ли в многообразии V. Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} F/V(R) & \xrightarrow{\tilde{\varphi}} & A \operatorname{wr}_V B \\ \downarrow & & \downarrow \\ F/R^2 & \xrightarrow{\hat{\varphi}} & (A/A^2) \operatorname{wr} B \end{array},$$

где вертикальные стрелки — естественные гомоморфизмы, $\hat{\varphi}$ — гомоморфизм из теоремы 1. С помощью диаграммы и теоремы 1 получаем, что гомоморфизм $\tilde{\varphi}$ переводит произвольную базу алгебры $R/\mathbf{V}(R)$ в множество элементов, линейно независимое по модулю T^2. В случае поля характеристики 0 система элементов V-свободной алгебры, линейно независимая по модулю коммутанта, порождает V-свободную алгебру. Поэтому ограничение $\tilde{\varphi}$ на $R/\mathbf{V}(R)$ является мономорфизмом. □

В дальнейшем будем считать, что $R \neq F$.

Следствие 1. *Если $|I| + |J| \geqslant 2$, то центр алгебры $F/\mathbf{V}(R)$ тривиален.*

Доказательство. Можно выделить 3 случая:

1) $|I| \geqslant 2$;
2) $|I| = 1$, $|J| \geqslant 1$;
3) $|I| = 0$, $|J| \geqslant 2$.

Приведем доказательство случая 1), остальные случаи рассматриваются аналогично. Итак, пусть $|I| \geqslant 2$; z — элемент, принадлежащий центру алгебры $F/\mathbf{V}(R)$; $\tilde{\varphi}(z) = b+t$, где $b \in B$, $t \in T$. Пусть i_1, i_2 — два различных элемента множества I. Выберем представитель b_{i_1}, принадлежащий алгебре B_{i_1}, и представитель b_{i_2}, принадлежащий алгебре B_{i_2}. Так как в $F/\mathbf{V}(R)$ выполняются равенства $[z, b_{i_1}] = 0$ и $[z, b_{i_2}] = 0$, то в T выполняются равенства

$$[b, ([a_{i_1}, b_{i_1}] + \cdots)] + [t, b_{i_1}] + [t, ([a_{i_1}, b_{i_1}] + \cdots)] = 0, \tag{3}$$

$$[b, ([a_{i_2}, b_{i_2}] + \cdots)] + [t, b_{i_2}] + [t, ([a_{i_2}, b_{i_2}] + \cdots)] = 0. \tag{4}$$

Напомним, что T — полиоднородная алгебра Ли относительно любой базы. Покажем, что $t = 0$.

Предположим, что $t \neq 0$ и однородная компонента t степени 1 равна 0. Обозначим через q наименьшую ненулевую компоненту t. Тогда из (3) следует, что $b = 0$, $[q, b_{i_1}] = 0$. Из последнего равенства нетрудно вывести, что $q = 0$. Противоречие.

Пусть $t \neq 0$, и однородная компонента t степени 1 не равна 0. Обозначим эту компоненту через q. Тогда справедливы равенства

$$[q, b_{i_1}] = [[a_{i_1}, b_{i_1}], b], \quad [q, b_{i_2}] = [[a_{i_2}, b_{i_2}], b].$$

Из этих равенств следует, что $q = 0$. Получаем противоречие.

Итак, мы привели к противоречию предположение о том, что $t \neq 0$. Значит, $t = 0$. Из равенства (3) нетрудно вывести, что $b = 0$. Применяя теорему 3, получаем $z = 0$. □

СПИСОК ЛИТЕРАТУРЫ

1. *Кукин Г. П.* О свободной лиевой сумме алгебр Ли с объединением// Алгебра и логика. — 1972. — *11*, № 1. — С. 59–86.
2. *Романовский Н. С.* О вложениях Шмелькина для абстрактных и проконечных групп// Алгебра и логика. — 1999. — *38*, № 5. — С. 598–612.
3. *Шмелькин А. Л.* Сплетения алгебр Ли и их применения в теории групп// Тр. Моск. мат. о-ва. — 1973. — *29*. — С. 247–260.
4. *Шмелькин А. Л.* Вложение в сплетение некоторых факторалгебр свободной суммы алгебр Ли// Зап. каф. высшей алгебры МГУ.