Новый тип размерностных многочленов от нескольких переменных, связанных с расширениями инверсных разностных полей

А. ЛЕВИН
Католический университет Америки, США
e-mail: levin@cua.edu

УДК 512.62

Ключевые слова: разностный многочлен, размерностный многочлен, редукция, эффективный порядок, характеристическое множество.

Аннотация

Мы представляем новый тип редукции инверсных разностных многочленов, который связан с разбиением базисного множества автоморфизмов σ и использует обобщение понятия эффективного порядка разностного многочлена. Затем мы развиваем соответствующий метод характеристических множеств и применяем его для установления существования и вычисления размерностных многочленов от нескольких переменных, которые выражают степени трансцендентности промежуточных полей конечно порождённого инверсного разностного расширения, порождённых трансформами образующих, порядки которых относительно данного разбиения σ ограничены сверху и снизу. Мы показываем, что новые разностные размерностные многочлены содержат существенно больше инвариантов расширения (т. е. числовых характеристик расширения, которые не зависят от системы его разностных образующих), чем стандартные разностные размерностные многочлены (с одним переменным). Мы также показываем, как полученные результаты могут быть применены к задаче об эквивалентности двух систем алгебраических разностных уравнений.

Abstract

A. Levin, New multivariate dimension polynomials of inversive difference field extensions, Fundamentalnaya i prikladnaya matematika, vol. 24 (2023), no. 4, pp. 143—169.

We introduce a new type of reduction of inversive difference polynomials associated with a partition of the basic set of automorphisms σ; we use a generalization of the concept of effective order of a difference polynomial. Then we develop the corresponding method of characteristic sets and apply it to prove the existence and obtain a method of computation of multivariate dimension polynomials of a new type that describe the transcendence degrees of intermediate fields of finitely generated inversive difference field extensions obtained by adjoining transforms of the generators whose orders with respect to the components of the partition of σ are bounded by two sequences of natural numbers. We show that such dimension polynomials carry essentially more invariants (that is, characteristics of the extension that do not depend on the set of its difference generators) than standard (univariate) difference dimension polynomials. We also show how the obtained results can be applied to the equivalence problem for systems of algebraic difference equations.

Фундаментальная и прикладная математика, 2023, том 24, № 4, с. 143—169.

1. Введение

Эта статья посвящена памяти моего дорогого учителя Александра Васильевича Михалёва, который внёс большой вклад во многие области математики, особенно в такие области современной алгебры, как теория колец, гомологическая алгебра, дифференциальная и разностная алгебра, компьютерная алгебра, алгебраическая K-теория, топологическая алгебра и теория кодирования. В своих работах по исследованию дифференциальных и разностных алгебраических структур [5, 6, 18—28, 28] Александр Васильевич получил значительное число фундаментальных результатов, относящимся к дифференциальным и разностным кольцам и модулям, характеристическим множествам дифференциальных и разностных многочленов, вычислительному анализу систем алгебраических дифференциальных и разностных уравнений. А. В. Михалёв был блестящим педагогом, его книги [6, 28] и обзорные статьи [25, 27] содержат глубокое и вместе с тем ясное изложение основных идей и методов современной дифференциальной и разностной алгебры. Особенно хочется отметить статью [26], в которой А. В. Михалёв и Е. В. Панкратьев открыли поразительную связь между дифференциальным размерностным многочленом Колчина [3] (см. также [4], где приведены многие свойства таких многочленов) и жёсткостью системы алгебраических дифференциальных уравнений — важной характеристикой такой системы, введённой А. Эйнштейном [2]. В [26] показано, что жёсткость системы алгебраических дифференциальных уравнений в смысле Эйнштейна выражается определённым дифференциальным размерностным многочленом, и указан способ вычисления этого многочлена с помощью методов характеристических множеств и базисов Грёбнера. Аналогичная интерпретация разностных размерностных многочленов и примеры вычислений жёсткости систем алгебраических разностных уравнений приведены в [6, раздел 6.4; 11; 12, раздел 7.7].

Кроме того, что разностный размерностный многочлен, связанный с системой алгебраических разностных уравнений, выражает жёсткость по Эйнштейну такой системы (важность понятия жёсткости для анализа систем уравнений математической физики объяснена в [2]), важная роль разностных размерностных многочленов определяется по крайней мере тремя другими факторами. Во-первых, разностный размерностный многочлен конечно порождённого расширения разностного поля (или системы разностных уравнений, определяющей такое расширение) несёт определённые инварианты расширения (соответственно системы уравнений), т. е. характеристики расширения, которые не меняются при переходе к другой системе разностных образующих (и соответствующей системе разностных уравнений на эти образующие) (см., например, [6, гл. 6; 12, гл. 4]. В этой связи следует упомянуть результаты о разностных размерностных многочленах от нескольких переменных, связанных с разбиениями базисного множества эндоморфизмов (см. [10; 11; 12, гл. 3; 14]. Эти многочлены содержат больше инвариантов соответствующего разностного расширения, чем разностные размерностные многочлены от одного переменного. (См. также [16], где результаты о размерностных многочленах от нескольких переменных обобщены на дифференциально-разностный случай.) Во-вторых, свойства разностных размерностных многочленов, связанных с простыми разностными идеалами в кольцах разностных многочленов дают важный инструмент для исследования размерности разностных алгебр (см. [6, гл. 7; 12, раздел 4.6; 15]. Наконец, результаты о разностных размерностных многочленах могут быть естественным образом обобщены на алгебраические и дифференциальные алгебраические структуры с действием конечно порождённых коммутативных групп (см. [13, 18, 20]).

В этой статье мы вводим понятие редукции инверсных разностных многочленов относительно фиксированного разбиения базисного множества автоморфизмов σ. Эта редукция учитывает эффективные порядки инверсных разностных многочленов относительно элементов разбиения множества σ (мы обобщаем понятие эффективного порядка, введённого в [1, гл. 2, раздел 4] в случае, когда множество σ состоит из одного элемента). Заметим, что идея использовать обобщённый эффективный порядок в случае неинверсных разностных многочленов впервые была использована в [17] для получения нового типа разностных размерностных многочленов от двух переменных. Здесь мы рассматриваем новый тип характеристических множеств, связанных с введённой редукцией, и применяем свойства этих характеристических множеств для доказательства существования размерностных многочленов от нескольких переменных, которые выражают степени трансцендентности промежуточных полей конечно порождённого инверсного разностного расширения, порождённых трансформами образующих, порядки которых относительно данного разбиения σ ограничены сверху и снизу. Полученные размерностные многочлены являются многочленами от $2p$ переменных, где p — число подмножеств в разбиении σ. Мы определяем инварианты полученных многочленов, т. е. числовые характеристики соответствующего расширения, которые содержатся в каждом его размерностном многочлене и которые не зависят от системы инверсных разностных образующих, с которой этот многочлен связан. Мы также показываем, что полученные размерностные многочлены содержат больше инвариантов соответствующего расширения инверсного разностного поля, чем размерностные многочлены от одного переменного, введённые в [9]. Заметим, что при изучении разностных алгебраических структур используются произведения положительных степеней базисных эндоморфизмов, а инверсные разностные кольца, поля и модули рассматриваются вместе с действием отображений, являющихся произведениями любых целых степеней базисных автоморфизмов. Поэтому, несмотря на то что теория размерности разностных колец и модулей во многом аналогична теории размерности соответствующих объектов дифференциальной алгебры, исследование инверсных разностных алгебраических структур (включая изучение размерностных характеристик таких структур) сталкивается со многими проблемами, обусловленными наличием отрицательных степеней базисных автоморфизмов.

2. Предварительные сведения

На протяжении всей статьи $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_{\leqslant 0}$ и $\mathbb{Q}$ обозначают соответственно множества всех неотрицательных целых чисел, всех неположительных целых чисел, целых чисел и рациональных чисел. Если S — конечное множество, то $\operatorname{Card} S$ обозначает число элементов множества S. Для любого положительного целого $m \leqslant_P$ обозначает порядок произведения на $\mathbb{N}^m$, т. е. частичный порядок, относительно которого $(a_1, \ldots, a_m) \leqslant_P (a'_1, \ldots, a'_m)$ тогда и только тогда, когда $a_i \leqslant a'_i$ для $i = 1, \ldots, m$. Лексикографический порядок будет обозначаться $\leqslant_{\text{lex}}$.

Под кольцом мы понимаем ассоциативное кольцо с единицей; гомоморфизм колец отображает единицу в единицу, мы предполагаем, что подкольцо содержит единицу кольца и что каждая алгебра над коммутативным кольцом унитарна. Предполагается, что все рассматриваемые поля имеют нулевую характеристику; $\mathbb{Q}[t_1, \ldots, t_p]$ обозначает кольцо многочленов от переменных $t_1, \ldots, t_p$ с рациональными коэффициентами.

Под *разностным кольцом* мы всегда понимаем коммутативное кольцо R, рассматриваемое вместе с конечным множеством $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ попарно коммутирующих инъективных эндоморфизмов кольца R, которое называется *базисным множеством* этого разностного кольца. Такое кольцо также называется σ-кольцом; если оно является полем, то мы говорим о *разностном поле* или σ-поле. Если все элементы базисного множества σ разностного кольца (поля) R являются его автоморфизмами, мы полагаем $\sigma^* = \{\alpha_1, \ldots, \alpha_m, \alpha_1^{-1}, \ldots, \alpha_m^{-1}\}$ и называем R *инверсным разностным кольцом* или σ^*-кольцом (соответственно *инверсным разностным полем* или σ^*-полем). В дальнейшем мы будем часто заменять слова «разностный» и «инверсный разностный» приставками σ- и σ^*- соответственно.

Если R — инверсное разностное кольцо с базисным множеством $\sigma = \{\alpha_1, \ldots, \alpha_m\}$, то Γ будет обозначать множество всех элементов $\gamma = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$ $(k_1, \ldots, k_m \in \mathbb{Z})$ свободной коммутативной группы, порождённой множеством σ. *Порядком* такого элемента γ называется число $\operatorname{ord} \gamma = \sum\limits_{i=1}^{m} |k_i|$; кроме того, для любого числа $r \in \mathbb{N}$ мы полагаем $\Gamma(r) = \{\gamma \in \Gamma \mid \operatorname{ord} \gamma \leqslant r\}$.

Подкольцо (идеал) R_0 σ-кольца R называется разностным подкольцом (или σ-подкольцом) кольца R (соответственно разностным идеалом или σ-идеалом) кольца R, если R_0 замкнуто относительно действия отображений из множества σ. σ-идеал I σ-кольца R называется *рефлексивным*, если включение $\alpha_i(a) \in I$ $(a \in R,\ \alpha_i \in \sigma)$ влечёт включение $a \in I$. Если σ-кольцо R инверсно, это свойство означает, что идеал I замкнут относительно действия автоморфизмов из множества σ^*. В этом случае мы говорим, что I — σ^*-идеал. Если σ-идеал (соответственно σ^*-идеал) P является простым (в обычном смысле), мы говорим, что P — простой σ-идеал (соответственно σ^*-идеал) кольца R.

Если R — σ-кольцо и $S \subseteq R$, то пересечение I всех σ-идеалов кольца R, содержащих S, т. е. наименьший σ-идеал кольца R, содержащий S, обозначается через $[S]$. Если множество S конечно, $S = \{a_1, \ldots, a_r\}$, мы говорим, что σ-идеал I конечно порождён (или σ-конечно порождён), и пишем $I = [a_1, \ldots, a_r]$. При этом элементы $a_1, \ldots, a_r$ называются σ-образующими σ-идеала I. Если σ-кольцо R инверсно, то наименьший σ^*-идеал кольца R, содержащий S, обозначается через $[S]^*$, а элементы множества S называются σ^*-образующими этого σ^*-идеала. Если $S = \{a_1, \ldots, a_r\}$, мы говорим, что σ^*-идеал $J = [S]^*$ конечно порождён (или σ^*-конечно порождён), и обозначаем это как $J = [a_1, \ldots, a_r]^*$. В этом случае J порождается как идеал множеством $\{\gamma(a) \mid a \in S,\ \gamma \in \Gamma\}$. (В дальнейшем мы часто будем писать γa вместо $\gamma(a)$.)

Если R — σ^*-кольцо, то выражение вида $\sum\limits_{\gamma \in \Gamma} a_\gamma \gamma$, где $a_\gamma \in R$ для любого $\gamma \in \Gamma$ и только конечное число коэффициентов a_γ отлично от нуля, называется *σ^*-оператором* над R. Это эндоморфизм аддитивной группы кольца R. Если $C = \sum\limits_{\gamma \in \Gamma} a_\gamma \gamma$ и $f \in R$, то $C(f) = \sum\limits_{\gamma \in \Gamma} a_\gamma \gamma(f)$. Два σ^*-оператора $\sum\limits_{\gamma \in \Gamma} a_\gamma \gamma$ и $\sum\limits_{\gamma \in \Gamma} b_\gamma \gamma$ считаются равными тогда и только тогда, когда $a_\gamma = b_\gamma$ для любого $\gamma \in \Gamma$. Множество всех σ^*-операторов над σ^*-кольцом R будет обозначаться через $\mathcal{E}_R$. Это множество обладает естественной структурой R-модуля; оно становится кольцом, если определить умножение его элементов по правилу $\gamma a = \gamma(a)\gamma$ для любых $a \in R$, $\gamma \in \Gamma$ и расширить это правило на умножение любых двух σ^*-операторов по дистрибутивности. Полученное кольцо называется кольцом σ^*-операторов над R. Ясно, что если I — σ^*-идеал кольца R, $I = [f_1, \ldots, f_k]^*$, то каждый элемент идеала I имеет вид $\sum\limits_{i=1}^{q} C_i(f_i)$ $(q \in \mathbb{N})$, где $C_1, \ldots, C_q \in \mathcal{E}_R$.

Если L — разностное поле (σ-поле) и K — его подполе, которое является σ-подкольцом поля L, мы говорим, что K — σ-подполе σ-поля L. При этом L называется σ-расширением или σ-надполем поля K. Мы также говорим, что имеем дело с σ-расширением L/K. Если σ-поле L инверсно и K — его σ-подполе, такое что $\alpha(K) \subseteq K$ для любого $\alpha \in \sigma^*$, мы говорим, что K — инверсное разностное подполе или σ^*-подполе σ^*-поля L. Мы также говорим, что имеем дело с σ^*-расширением L/K. При этом если $S \subseteq K$, то наименьшее σ^*-подполе поля L, содержащее K и S, обозначается $K\langle S\rangle^*$, а S называется множеством *σ^*-образующих* $K\langle S\rangle^*$ над K. Если множество S конечно, $S = \{\eta_1, \ldots, \eta_n\}$, говорят, что L/K — конечно порождённое инверсное разностное расширение (или σ^*-расширение). Как поле $L\langle S\rangle^*$ равно $K(\gamma a \mid \gamma \in \Gamma,\ a \in S)$.

Пусть R и R' — два разностных кольца с одним и тем же базисным множеством σ. (Более точно, мы предполагаем, что имеются отображения множества σ во множества эндоморфизмов колец R и R', такие что образы любых двух элементов $\alpha, \beta \in \sigma$ коммутируют. Для удобства мы обозначаем эти образы теми же символами α и β.) Гомоморфизм колец $\varphi\colon R \to R'$ называется *разностным гомоморфизмом* (или *σ-гомоморфизмом*), если $\varphi(\alpha a) = \alpha\varphi(a)$ для любых $\alpha \in \sigma$, $a \in R$. Легко видеть, что ядро такого отображения является рефлексивным разностным идеалом кольца R.

В дальнейшем мы будем иметь дело с инверсными кольцами и полями (σ^*-кольцами и σ^*-полями). Если R — σ^*-кольцо и $Y = \{y_1, \ldots, y_n\}$ — конечное множество символов, мы можем рассматривать кольцо многочленов $R[\Gamma Y]$, где ΓY обозначает множество символов $\{\gamma y_j \mid \gamma \in \Gamma,\ 1 \leqslant j \leqslant n\}$, как σ^*-кольцо, содержащее R в качестве своего σ^*-подкольца. При этом структура σ^*-кольца на $R[\Gamma Y]$ определяется правилом $\alpha(\gamma y_j) = (\alpha\gamma)y_j$ для любых $\alpha \in \sigma^*$, $\gamma \in \Gamma$, $1 \leqslant j \leqslant n$. Полученное σ^*-кольцо называется кольцом инверсных разностных многочленов (или σ^*-многочленов) от σ^*-неизвестных $y_1, \ldots, y_n$ над R. σ^*-идеал кольца $R\{y_1, \ldots, y_n\}^*$ называется *линейным*, если он порождён (как σ^*-идеал) однородными линейными σ^*-многочленами, т. е. многочленами вида $\sum\limits_{i=1}^{d} a_i\gamma_i y_{k_i}$ ($a_i \in R$, $\gamma_i \in \Gamma$, $1 \leqslant k_i \leqslant n$ при $i = 1, \ldots, d$). Как показано в [12, утверждение 2.4.9], если R — σ^*-поле, то каждый линейный σ^*-идеал кольца $R\{y_1, \ldots, y_n\}^*$ является простым.

Если K — инверсное разностное поле (σ^*-поле), $f \in K\{y_1, \ldots, y_n\}^*$ и $\eta = (\eta_1, \ldots, \eta_n)$ — n-мерный вектор, координаты которого лежат в некотором σ^*-надполе поля K, то $f(\eta)$ (или $f(\eta_1, \ldots, \eta_n)$) обозначает результат замены в f каждого вхождения γy_i на элемент $\gamma\eta_i$ ($\gamma \in \Gamma$, $1 \leqslant i \leqslant n$).

Если $\pi\colon R = K\{y_1, \ldots, y_n\}^* \to L = K\langle\eta_1, \ldots, \eta_n\rangle^*$ — естественный кольцевой σ-гомоморфизм ($\pi(a) = a$ для любых $a \in K$ и $y_i \mapsto \eta_i$), то $P = \operatorname{Ker}\pi$ — простой σ^*-идеал кольца R, который называется *определяющим идеалом* расширения L/K. В этом случае σ^*-поле L изоморфно σ^*-полю частных $\operatorname{qf}(R/P)$ инверсного разностного фактор-кольца R/P относительно σ-изоморфизма, при котором $\eta_i \mapsto y_i + P$ ($1 \leqslant i \leqslant n$).

Пусть K — σ^*-поле и $\mathcal{U}$ — семейство элементов из некоторого σ^*-надполя поля K. Говорят, что семейство $\mathcal{U}$ *σ-алгебраически зависимо* над K, если семейство $\Gamma\mathcal{U} = \{\gamma(u) \mid \gamma \in \Gamma,\ u \in \mathcal{U}\}$ алгебраически зависимо над K, т. е. существуют элементы $u_1, \ldots, u_k \in \Gamma\mathcal{U}$ и ненулевой многочлен f от k переменных, такой что $f(u_1, \ldots, u_k) = 0$. В противном случае мы говорим, что семейство $\mathcal{U}$ *σ-алгебраически независимо* над K.

Если L — σ^*-надполе σ^*-поля K, то множество $B \subseteq L$ называется *σ-базисом трансцендентности* поля L над K (или расширения L/K), если это множество σ-алгебраически независимо над K и каждый элемент $a \in L$ σ-алгебраичен над $K\langle B\rangle^*$ (это означает, что множество $\{\gamma a \mid \tau \in \Gamma\}$ алгебраически зависимо над полем $K\langle B\rangle^*$). Если L — конечно порождённое σ^*-расширение σ^*-поля K, то все σ-базисы трансцендентности L над K конечны и содержат одинаковое число элементов (см. [12, утверждение 4.1.6]). Это число называется *разностной степенью трансцендентности* (или *σ-степенью трансцендентности*) поля L над K (или расширения L/K); оно обозначается через $\sigma\text{-}\operatorname{tr.deg}_K L$.

Следующая теорема, доказательство которой приведено в [6, раздел 6.4], представляет размерностный многочлен от одного переменного, связанного с конечно порождённым расширением инверсного разностного поля.

Теорема 2.1. *Пусть K — инверсное разностное поле с базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_m\}$ и $L = K\langle\eta_1, \dots, \eta_n\rangle^*$ — σ^*-расширение поля K, порождённое конечным множеством $\eta = \{\eta_1, \dots, \eta_n\}$. Тогда существует многочлен $\varphi_{\eta|K}(t) \in \mathbb{Q}[t]$, такой что*

1) $\varphi_{\eta|K}(r) = \operatorname{tr.deg}_K K(\{\gamma\eta_j \mid \gamma \in \Gamma(r),\ 1 \leqslant j \leqslant n\})$ *для всех достаточно больших* $r \in \mathbb{N}$;
2) $\deg \varphi_{\eta|K} \leqslant m$ *и многочлен* $\varphi_{\eta|K}(t)$ *может быть представлен в виде*
$$\varphi_{\eta|K}(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i},$$
где $a_0, \dots, a_m \in \mathbb{Z}$ и $2^m \mid a_m$;
3) $d = \deg \varphi_{\eta|K}$, a_m *и* a_d *не зависит от множества* η σ^*-*образующих расширения* L/K ($a_d \neq a_m$ *тогда и только тогда, когда* $d < m$). *Кроме того,* $\frac{a_m}{2^m} = \sigma\text{-}\operatorname{tr.deg}_K L$;
4) *если элементы* $\eta_1, \dots, \eta_n$ σ-*алгебраически независимы над* K, *то*
$$\varphi_{\eta|K}(t) = n \sum_{k=0}^{m} (-1)^{m-k} 2^k \binom{n}{k} \binom{t+k}{k}.$$

Многочлен $\varphi_{\eta|K}(t)$ называется *σ^*-размерностным многочленом* расширения L/K, связанным с системой σ^*-образующих η. Методы и алгоритмы вычисления таких многочленов приведены в [6].

Размерностные многочлены подмножеств множества $\mathbb{Z}^m$

Ниже мы приводим некоторые результаты о целозначных многочленах, связанных с подмножествами множества $\mathbb{Z}^m$ ($m \in \mathbb{Z}$, $m > 0$). Доказательства соответствующих утверждений можно найти в [5; 6, гл. 2].

Определение 2.2. Многочлен от p переменных $f(t_1, \dots, t_p) \in \mathbb{Q}[t_1, \dots, t_p]$ называется *целозначным*, если $f(r_1, \dots, r_p) \in \mathbb{Z}$ для всех достаточно больших $(r_1, \dots, r_p) \in \mathbb{N}^p$. (Это означает, что существуют $s_1, \dots, s_p \in \mathbb{N}$, такие что $f(r_1, \dots, r_p) \in \mathbb{Z}$ для всех элементов $(r_1, \dots, r_p) \in \mathbb{N}^p$, для которых $r_1 \geqslant s_1, \dots, r_p \geqslant s_p$.)

Ясно, что каждый многочлен с целыми коэффициентами является целозначным. Примером целозначного многочлена от p переменных с нецелыми коэффициентами ($p \in \mathbb{N}$, $p \geqslant 1$) может служить многочлен $\prod_{i=1}^{p} \binom{t_i}{m_i}$, где $m_1, \dots, m_p \in \mathbb{N}$. (Как обычно, $\binom{t}{k} = \frac{t(t-1)\dots(t-k+1)}{k!}$ при $k \in \mathbb{Z}$, $k \geqslant 1$, $\binom{t}{0} = 1$ и $\binom{t}{k} = 0$, если $k < 0$.) Следующая теорема, доказанная в [6, гл. 2], даёт «каноническое» представление целозначного многочлена от нескольких переменных.

Теорема 2.3. *Пусть $f(t_1, \dots, t_p)$ — целозначный многочлен от p переменных $t_1, \dots, t_p$, и пусть $\deg_{t_i} f = m_i$ ($1 \leqslant i \leqslant p$), где $m_1, \dots, m_p \in \mathbb{N}$. Тогда многочлен*

$f(t_1,\dots,t_p)$ может быть представлен в виде

$$f(t_1,\dots,t_p)=\sum_{i_1=0}^{m_1}\dots\sum_{i_p=0}^{m_p}a_{i_1\dots i_p}\binom{t_1+i_1}{i_1}\dots\binom{t_p+i_p}{i_p} \tag{1}$$

с однозначно определёнными целыми коэффициентами $a_{i_1\dots i_p}$ $(0\leqslant i_k\leqslant m_k$ при $k=1,\dots,p)$.

Ниже мы имеем дело с подмножествами множества $\mathbb{Z}^m$ $(m\in\mathbb{Z},\ m>0)$. Кроме того, мы зафиксируем разбиение множества $\mathbb{N}_m=\{1,\dots,m\}$ на попарно непересекающиеся подмножества:

$$\mathbb{N}_m=\Delta_1\cup\Delta_2\cup\ldots\cup\Delta_p\quad(p\geqslant 1), \tag{2}$$

где

$$\Delta_1=\{1,\dots,m_1\},\Delta_2=\{m_1+1,\dots,m_1+m_2\},\dots,\Delta_p=\{m_1+\ldots+m_{p-1}+1,\dots,m\},$$

$$m_i=\operatorname{Card}\Delta_i\quad(1\leqslant i\leqslant p),\quad\sum_{i=1}^{p}m_i=m.$$

Если $a=(a_1,\dots,a_m)\in\mathbb{Z}^m$, то числа

$$\sum_{i=1}^{m_1}|a_i|,\ \sum_{i=m_1+1}^{m_1+m_2}|a_i|,\dots,\sum_{i=m_1+\ldots+m_{p-1}+1}^{m}|a_i|$$

будут обозначаться как $\operatorname{ord}_1 a,\dots,\operatorname{ord}_p a$ соответственно. Будем называть $\operatorname{ord}_k a$ $(1\leqslant k\leqslant p)$ *порядком элемента a относительно* Δ_k. Кроме того, мы фиксируем представление множества $\mathbb{Z}^n$ в виде объединения

$$\mathbb{Z}^m=\bigcup_{1\leqslant j\leqslant 2^m}\mathbb{Z}_j^{(m)}, \tag{3}$$

где $\mathbb{Z}_1^{(m)},\dots,\mathbb{Z}_{2^m}^{(m)}$ — все различные декартовы произведения m множеств, каждое из которых является либо $\mathbb{N}$, либо $\mathbb{Z}_{\leqslant 0}$. Мы предполагаем, что $\mathbb{Z}_1^{(m)}=\mathbb{N}$, и говорим, что $\mathbb{Z}_j^{(m)}$ — *j-й ортант* множества $\mathbb{Z}^m$ $(1\leqslant j\leqslant 2^m)$.

Мы будем рассматривать $\mathbb{Z}^m$ как частично упорядоченное множество с порядком $\trianglelefteq$, таким что $(e_1,\dots,e_m)\trianglelefteq(e'_1,\dots,e'_m)$ тогда и только тогда, когда $(e_1,\dots,e_m)$ и $(e'_1,\dots,e'_m)$ лежат в одном и том же ортанте и $(|e_1|,\dots,|e_m|)\leqslant_P(|e'_1|,\dots,|e'_m|)$.

Если $A\subseteq\mathbb{Z}^m$, то W_A будет обозначать множество всех тех элементов множества $\mathbb{Z}^m$, которые не превосходят ни одного элемента $a\in A$ относительно порядка $\trianglelefteq$. Кроме того, для любых $r_1,\dots,r_p\in\mathbb{N}$ $A(r_1,\dots,r_p)$ будет обозначать множество всех элементов $x=(x_1,\dots,x_m)\in A$, удовлетворяющих условиям $\operatorname{ord}_i x\leqslant r_i$ $(i=1,\dots,p)$.

Введённые выше обозначения могут быть естественным образом применены к подмножествам множества $\mathbb{N}^m$ (рассматриваемого как подмножество $\mathbb{Z}^m$). Если $E\subseteq\mathbb{N}^m$ и $s_1,\dots,s_p\in\mathbb{N}$, то $E(s_1,\dots,s_p)$ будет обозначать множество всех m-мерных точек $e \in E$, таких что $\operatorname{ord}_i e \leqslant s_i$ $(i = 1, \dots, p)$. Кроме того, с каждым множеством $E \subseteq \mathbb{N}^m$ мы свяжем множество

$$V_E = \{v \in \mathbb{N}^m \mid a \nleq v \text{ для любого элемента } a \in E\}.$$

(Таким образом, $(e_1, \dots, e_m) \in V_E$ тогда и только тогда, когда существует $i \in \in \{1, \dots, m\}$, такое что $e_i > v_i$.) Следующие две теоремы, доказанные в [6, гл. 2] обобщают известный результат Колчина о целозначных многочленах от одной переменной, связанных с подмножествами множества $\mathbb{N}^m$ (см. [4, гл. 0, лемма 16]), и дают формулы для вычисления целозначных многочленов от нескольких переменных, связанных с подмножествами множеств $\mathbb{N}^m$ и $\mathbb{Z}^m$.

Теорема 2.4. *Пусть $E \subseteq \mathbb{N}^m$. Тогда при фиксированном разбиении* (2) *множества $\mathbb{N}_m$ существует целозначный многочлен $\omega_E(t_1, \dots, t_p)$ со следующими свойствами*:

1) *для всех достаточно больших $(r_1, \dots, r_p) \in \mathbb{N}^p$*

$$\omega_E(r_1, \dots, r_p) = \operatorname{Card} V_A(r_1, \dots, r_p);$$

2) *полная степень $\deg \omega_E$ многочлена ω_E не превосходит m и $\deg_{t_i} \omega_E \leqslant m_i$ $(1 \leqslant i \leqslant p)$;*

3) $\deg \omega_E = m$ *тогда и только тогда, когда $E = \varnothing$. В этом случае*

$$\omega_E(t_1, \dots, t_p) = \prod_{i=1}^{p} \binom{t_i + m_i}{m_i}.$$

Определение 2.5. Многочлен $\omega_E(t_1, \dots, t_p)$ называется размерностным многочленом множества $E \subseteq \mathbb{N}^m$, связанным с разбиением (2) множества $\mathbb{N}_m$.

Теорема 2.6. *Пусть $E = \{e_1, \dots, e_q\}$ $(q \geqslant 1)$ — конечное подмножество множества $\mathbb{N}^m$, и пусть разбиение* (2) *множества $\mathbb{N}_m$ фиксировано. Пусть $e_i = (e_{i1}, \dots, e_{im})$ $(1 \leqslant i \leqslant q)$, и для каждого $l \in \mathbb{N}$, $0 \leqslant l \leqslant q$, пусть $\Theta(l, q)$ обозначает множество всех l-элементных подмножеств множества $\mathbb{N}_q = \{1, \dots, q\}$. Пусть $\bar{e}_{\varnothing j} = 0$, и для каждого $\theta \in \Theta(l, q)$, $\theta \neq \varnothing$, пусть $\bar{e}_{\theta j} = \max\{e_{ij} \mid i \in \theta\}$ $(1 \leqslant j \leqslant m)$. Кроме того, пусть $b_{\theta k} = \sum\limits_{h \in \Delta_k} \bar{e}_{\theta h}$ $(k = 1, \dots, p)$. Тогда*

$$\omega_E(t_1, \dots, t_p) = \sum_{l=0}^{q} (-1)^l \sum_{\theta \in \Theta(l,q)} \prod_{j=1}^{p} \binom{t_j + m_j - b_{\theta j}}{m_j}. \tag{4}$$

Замечание 2.7. Легко видеть, что если $E \subseteq \mathbb{N}^m$ and E^* — множество всех минимальных элементов множества E относительно порядка произведения, то множество E^* конечно и $\omega_E(t_1, \dots, t_p) = \omega_{E^*}(t_1, \dots, t_p)$. Поэтому теорема 2.6 даёт алгоритм, позволяющий вычислить размерностный многочлен любого подмножества множества $\mathbb{N}^m$ (при фиксированном разбиении (2) множества $\mathbb{N}_m$): мы сначала находим множество минимальных элементов данного подмножества, а потом применяем теорему 2.6.

Следующая теорема, доказанная в [6, раздел 2.5], даёт аналог результатов теорем 2.4—2.6 для подмножеств множества $\mathbb{Z}^m$.

Теорема 2.8. *Пусть* $A \subseteq \mathbb{Z}^m$. *Тогда при фиксированном разбиении* (2) *множества* $\mathbb{N}_m$ *существует целозначный многочлен от* p *переменных* $\varphi_A(t_1, \dots, t_p)$, *такой что*

1) *для всех достаточно больших* $(r_1, \dots, r_p) \in \mathbb{N}^p$
$$\varphi_A(r_1, \dots, r_p) = \operatorname{Card} W_A(r_1, \dots, r_p);$$
2) $\deg \varphi_A \leqslant m$ *и* $\deg_{t_i} \varphi_A \leqslant m_i$ $(i = 1, \dots, p)$. *Кроме того, если многочлен* $\varphi_A(t_1, \dots, t_p)$ *представлен в виде* (1), *то* $2^m \mid a_{m_1 \dots m_p}$;
3) *рассмотрим отображение* $\rho\colon \mathbb{Z}^m \to \mathbb{N}^{2m}$, *такое что если* $e = (e_1, \dots, e_m)$, *то*
$$\rho(e) = (\max\{e_1, 0\}, \dots, \max\{e_m, 0\}, \max\{-e_1, 0\}, \dots, \max\{-e_m, 0\}).$$
Пусть $B = \rho(A) \cup \{\bar{e}_1, \dots, \bar{e}_m\}$, *где* $\bar{e}_i$ $(1 \leqslant i \leqslant m)$ — *элемент множества* $\mathbb{N}^{2m}$, i*-я и* $(m+i)$*-я координаты которого равны* 1, *а все остальные координаты — нули. Тогда*
$$\varphi_A(t_1, \dots, t_p) = \omega_B(t_1, \dots, t_p),$$
где $\omega_B(t_1, \dots, t_p)$ — *размерностный многочлен множества* B (*см. определение* 2.5), *связанный со следующим разбиением множества* $\mathbb{N}_{2m}$: $\mathbb{N}_{2m} = \Delta'_1 \cup \Delta_2 \cup \ldots \cup \Delta'_p$, *где* $\Delta'_i = \Delta_i \cup \{m + k \mid k \in \Delta_i\}$ *при* $i = 1, \dots, p$ (*см. разбиение* (2));
4) *если* $A = \varnothing$, *то*
$$\varphi_A(t_1, \dots, t_p) = \prod_{j=1}^{p} \left[\sum_{i=0}^{m_j} (-1)^{m_j - i} 2^i \binom{m_j}{i} \binom{t_j + i}{i} \right]. \tag{5}$$

Определение 2.9. Многочлен $\varphi_A(t_1, \dots, t_p)$ называется размерностным многочленом множества $A \subseteq \mathbb{N}^m$, связанным с разбиением (2) множества $\mathbb{N}_m$.

Замечание 2.10. Равенство (5) (как и последняя часть теоремы 2.1) вытекает из того факта, что число решений $(x_1, \dots x_m) \in \mathbb{Z}^m$ неравенства $|x_1| + \ldots + |x_m| \leqslant r$ $(r \in \mathbb{N})$ равно $\sum\limits_{k=0}^{m} (-1)^{m-k} 2^k \binom{n}{k} \binom{r+k}{k}$ (см. [6, утверждение 2.1.9]). Следовательно, если $r_1, \dots, r_p, s_1, \dots, s_p \in \mathbb{N}$, $s_i < r_i$ $(1 \leqslant i \leqslant p)$ и
$$B = \left\{ b = (b_1, \dots, b_m) \in \mathbb{Z}^m \;\middle|\; s_i \leqslant \sum_{\nu \in \Delta_i} |b_\nu| \leqslant r_i \text{ для } i = 1, \dots, p \right\}$$
(разбиение (2) фиксировано), то
$$\operatorname{Card} B = \prod_{i=1}^{p} \left[\sum_{j=0}^{m_i} (-1)^{m_i - j} 2^j \binom{m_i}{j} \left(\binom{r_i + j}{j} - \binom{s_i + j - 1}{j} \right) \right].$$

Мы используем это замечание при доказательстве теоремы 4.1.

3. E-редукция инверсных разностных многочленов. E-характеристические множества

Пусть K — инверсное разностное поле с базисным множеством $\sigma = \{\alpha_1, \ldots, \alpha_m\}$. Зафиксируем разбиение множества σ, т. е. представление этого множества в виде объединения попарно непересекающихся подмножеств:

$$\sigma = \sigma_1 \cup \ldots \cup \sigma_p \tag{6}$$

где

$$\sigma_1 = \{\alpha_1, \ldots, \alpha_{m_1}\},\ \sigma_2 = \{\alpha_{m_1+1}, \ldots, \alpha_{m_1+m_2}\}, \ldots,$$
$$\sigma_p = \{\alpha_{m_1+\ldots+m_{p-1}+1}, \ldots, \alpha_m\} \quad (m_1 + \ldots + m_p = m).$$

Если $\gamma = \alpha_1^{k_1} \ldots \alpha_m^{k_m} \in \Gamma$ ($k_i \in \mathbb{Z}$), то *порядком элемента* γ *относительно множества* σ_i ($1 \leqslant i \leqslant p$) будем называть число $\sum\limits_{\nu=m_1+\ldots+m_{i-1}+1}^{m_1+\ldots+m_i} |k_\nu|$, обозначая его $\operatorname{ord}_i \gamma$. (Если $i = 1$, то последняя сумма заменяется на $\sum\limits_{\nu=1}^{m_1} |k_\nu|$.) Кроме того, для любых $r_1, \ldots, r_p \in \mathbb{N}$ мы полагаем

$$\Gamma(r_1, \ldots, r_p) = \{\gamma \in \Gamma \mid \operatorname{ord}_i \gamma \leqslant r_i,\ i = 1, \ldots, p\}.$$

Мы также будем рассматривать p линейных порядков $<_1, \ldots, <_p$ на группе Γ, таких что

$$\gamma = \alpha_1^{k_1} \ldots \alpha_m^{k_m} <_i \gamma' = \alpha_1^{k'_1} \ldots \alpha_m^{k'_m} \quad (1 \leqslant i \leqslant p)$$

тогда и только тогда, когда $(2m + p)$-мерная точка

$$\begin{aligned}(&\operatorname{ord}_i \gamma, \operatorname{ord}_1 \gamma, \ldots, \operatorname{ord}_{i-1} \gamma, \operatorname{ord}_{i+1} \gamma, \ldots, \operatorname{ord}_p \gamma,\\ &|k_{m_1+\ldots+m_{i-1}+1}|, \ldots, |k_{m_1+\ldots+m_i}|, k_{m_1+\ldots+m_{i-1}+1}, \ldots, k_{m_1+\ldots+m_i},\\ &|k_1|, \ldots, |k_{m_1+\ldots+m_{i-1}}|, |k_{m_1+\ldots+m_i+1}|, \ldots, |k_m|,\\ &k_1, \ldots, k_{m_1+\ldots+m_{i-1}}, k_{m_1+\ldots+m_i+1}, \ldots, k_m)\end{aligned}$$

меньше, чем соответствующая $(2m + p)$-мерная точка для γ' относительно лексикографического порядка на $\mathbb{Z}^{2m+p}$.

Два элемента $\gamma_1 = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$ и $\gamma_2 = \alpha_1^{l_1} \ldots \alpha_n^{l_m}$ группы Γ называются *подобными*, если $(k_1, \ldots, k_m)$ и $(l_1, \ldots, l_m)$ лежат в одном и том же ортанте множества $\mathbb{Z}^m$ (см. (3)). В этом случае мы пишем $\gamma_1 \sim \gamma_2$. Мы говорим, что γ_1 *делит* γ_2 (или что γ_2 является *трансформой* элемента γ_1) и пишем $\gamma_1 \mid \gamma_2$, если существует элемент $\gamma \in \Gamma$, такой что $\gamma \sim \gamma_1$ и $\gamma_2 = \gamma\gamma_1$.

Пусть $R = K\{y_1, \ldots, y_n\}^*$ — алгебра σ^*-многочленов от n σ^*-неизвестных $y_1, \ldots, y_n$ над K. Мы можем рассматривать R как кольцо многочленов от множества переменных $\Gamma Y = \{\gamma y_i \mid \gamma \in \Gamma,\ 1 \leqslant i \leqslant n\}$; элементы этого множества будут называться *термами*. Мы определяем порядок терма $u = \gamma y_i$ ($\gamma \in \Gamma$, $1 \leqslant i \leqslant n$) относительно множества σ_j ($1 \leqslant j \leqslant n$) как соответствующий порядок элемента γ и обозначаем его $\operatorname{ord}_j u$. Кроме того, рассматривая представление (3) множества $\mathbb{Z}^m$ в виде объединения ортантов $\mathbb{Z}_j^m$, мы полагаем

$$\Gamma_j = \{\alpha_1^{k_1} \ldots \alpha_m^{k_m} \in \Gamma \mid (k_1, \ldots, k_m) \in \mathbb{Z}_j^m\}$$

и

$$\Gamma_j Y = \{\gamma y_i \mid \gamma \in \Gamma_j,\ 1 \leqslant i \leqslant n\}.$$

Назовём два терма $u = \gamma y_i$ и $v = \gamma' y_j$ *подобными*, если $\gamma \sim \gamma'$; в этом случае мы пишем $u \sim v$. Если $u = \gamma y_i$ — терм, $\gamma' \in \Gamma$ и $\gamma \sim \gamma'$, мы говорим, что u и γ' подобны и пишем $u \sim \gamma'$. Ясно, что если $u \in \Gamma Y$, $\gamma \in \Gamma$ и $\gamma \sim u$, то $\operatorname{ord}_j(\gamma u) = \operatorname{ord}_j \gamma + \operatorname{ord}_j u$ $(j = 1, \ldots, p)$. Если $u, v \in \Gamma Y$, мы говорим, что *u делит v* (или что *v — трансформа* терма u), и пишем $u \mid v$, если $u = \gamma' y_i$, $v = \gamma'' y_i$ для некоторого y_i и $\gamma' \mid \gamma''$. (Если $\gamma'' = \gamma\gamma'$, где $\gamma \in \Gamma$ и $\gamma \sim \gamma'$, мы обозначаем γ как $\frac{v}{u}$).

Мы будем рассматривать p порядков $<_1, \ldots, <_p$ на множестве ΓY, которые соответствуют порядкам введённым на группе Γ (мы используем те же символы для обозначения порядков на Γ и ΓY). Эти порядки определяются следующим условием: $\gamma y_j <_i \gamma' y_k$ тогда и только тогда, когда $\gamma <_i \gamma'$ в Γ или $\gamma = \gamma'$ и $j < k$ $(1 \leqslant i \leqslant p,\ 1 \leqslant j, k \leqslant n)$.

Определение 3.1. Пусть $f \in K\{y_1, \ldots, y_n\}^* \setminus K$ и $1 \leqslant k \leqslant p$. Тогда наибольший терм σ^*-многочлена f относительно порядка $<_k$ называется *k-лидером* этого σ^*-многочлена; он обозначается через $u_f^{(k)}$. Наименьший терм σ^*-многочлена f относительно $<_k$ называется *k-колидером* этого σ^*-многочлена и обозначается через $v_f^{(k)}$.

Определение 3.2. Пусть $f \in K\{y_1, \ldots, y_n\}^*\} \setminus K$, и пусть $u_f^{(k)} = \alpha_1^{k_1} \ldots \alpha_m^{k_m} y_i$ и $v_f^{(k)} = \alpha_1^{l_1} \ldots \alpha_m^{l_m} y_j$ — k-лидер и k-колидер σ^*-многочлена f соответственно. Тогда число $\operatorname{ord}_k u_f^{(k)} - \operatorname{ord}_k v_f^{(k)} \in \mathbb{N}$ называется *k-м эффективным порядком* σ^*-многочлена f; он обозначается через $\operatorname{Eord}_k f$.

Определение 3.3. Пусть f, g — два σ^*-многочлена из кольца $K\{y_1, \ldots, y_n\}^*$. Мы говорим, что *ранг f ниже, чем ранг g*, и пишем $\operatorname{rk} f < \operatorname{rk} g$, если $f \in K$, $g \notin K$ или

$$\begin{aligned}\bigl(u_f^{(1)}, \deg_{u_f^{(1)}} f, \operatorname{ord}_2 u_f^{(2)}, \ldots, \operatorname{ord}_p u_f^{(p)}, \operatorname{Eord}_1 f, \ldots, \operatorname{Eord}_p f\bigr) <_{\text{lex}}& \\ <_{\text{lex}} \bigl(u_g^{(1)}, \deg_{u_g^{(1)}} f, \operatorname{ord}_2 u_g^{(2)}, \ldots, \operatorname{ord}_p u_g^{(p)}, \operatorname{Eord}_1 g, \ldots, \operatorname{Eord}_p g\bigr)& \qquad (7)\end{aligned}$$

(элементы $u_f^{(1)}$ и $u_g^{(1)}$ сравниваются относительно порядка $<_1$ на множестве термов ΓY). Если последние две $(2p + 1)$-мерные точки равны (или $f, g \in K$), мы говорим, что f и g имеют один и тот же ранг, и пишем $\operatorname{rk} f = \operatorname{rk} g$.

Определение 3.4. Пусть $f, g \in K\{y_1, \ldots, y_n\}^*$ и $d = \deg_{u_g^{(1)}} g$. Мы говорим, что f *E-редуцирован* относительно g, если выполнено одно из следующих двух условий:

1) f не содержит никакой степени терма $\bigl(\gamma u_g^{(1)}\bigr)^e$ $(\gamma \in \Gamma)$, такой что $\gamma \sim u_g^{(1)}$ и $e \geqslant d$;
2) f содержит степень терма $\bigl(\gamma u_g^{(1)}\bigr)^e$, в которой $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$ и $e \geqslant d$, но при этом либо существует $k \in \mathbb{N}_p$, $k \geqslant 2$, такое что $\operatorname{ord}_k u_{\gamma g}^{(k)} > \operatorname{ord}_k(u_f^{(k)})$, либо существует $j \in \mathbb{N}_p$, такое что $\operatorname{ord}_j v_{\gamma g}^{(j)} < \operatorname{ord}_j(v_f^{(j)})$. (Допускается, что выполняются оба последних условия.)

Таким образом, f не является E-редуцированным относительно g, если f содержит терм вида $\bigl(\gamma u_g^{(1)}\bigr)^e$, такой что $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$, $e \geqslant d = \deg_{u_g^{(1)}} g$ и $\operatorname{ord}_k u_{\gamma g}^{(k)} \leqslant \operatorname{ord}_k\bigl(u_f^{(k)}\bigr)$ $(k = 2, \ldots, p)$, $\operatorname{ord}_j v_{\gamma g}^{(j)} \geqslant \operatorname{ord}_j\bigl(v_f^{(j)}\bigr)$ $(j = 1, \ldots p)$.

Замечание 3.5. Если $f, g \in K\{y_1, \ldots, y_n\}^*$, то f редуцирован относительно g в смысле [6, определение 3.4.22] применительно к порядку $<_1$, если выполняется первое условие определения 3.4. Ясно, что в этом случае f E-редуцирован относительно g.

Замечание 3.6. Из [29, лемма 3.3] следует, что если $f \in R = K\{y_1, \ldots, y_n\}^*$, $j \in \{1, \ldots, 2^m\}$ и $k \in \{1, \ldots, p\}$, то f содержит некоторые термы u_{fjk} и v_{fjk}, такие что для всех элементов $\gamma = \alpha_1^{k_1} \ldots \alpha_m^{k_m} \in \Gamma_j$ с достаточно большим $(|k_1|, \ldots, |k_m|) \in \mathbb{N}^m$ (в смысле определения 2.2) мы имеем $u_{\gamma f}^{(k)} = \gamma u_{fjk}$ и $v_{\gamma f}^{(k)} = \gamma v_{fjk}$. Например, пусть $\sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ рассматривается вместе с разбиением $\sigma = \sigma_1 \cup \sigma_2 \cup \sigma_3$, где $\sigma_i = \{\alpha_i\}$ $(i = 1, 2, 3)$,

$$f = \alpha_1^2 \alpha_2^{-1} \alpha_3^{-3} y + \alpha_1^{-3} \alpha_2 \alpha_3^{-4} y + \alpha_1 \alpha_2^{-2} \alpha_3^2 y + \alpha_1^2 \alpha_2^2 \alpha_3 y \in K\{y\}^*,$$

и пусть j соответствует ортанту $\mathbb{Z}_j^{(3)} = \{(k_1, k_2, k_3) \mid k_1 \leqslant 0,\ k_2 \geqslant 0,\ k_3 \leqslant 0\}$. Тогда для любого $\gamma = \alpha_1^{-r} \alpha_2^s \alpha_3^{-t} \in \Gamma_j$ $(r, s, t \geqslant 0)$ мы будем иметь

$$\gamma f = \alpha_1^{-r+2} \alpha_2^{s-1} \alpha_3^{-t-3} y + \alpha_1^{-r-3} \alpha_2^{s+1} \alpha_3^{-t-4} y + \\ + \alpha_1^{-r+1} \alpha_2^{s-2} \alpha_3^{-t+2} y + \alpha_1^{-r+2} \alpha_2^{s+} \alpha_3^{-t+1} y,$$

так что $u_{j1f} = u_{j3f} = \alpha_1^{-3} \alpha_2 \alpha_3^{-4} y$, $u_{j2f} = v_{j1f} = \alpha_1^2 \alpha_2^2 \alpha_3 y$ и $v_{j2f} = v_{j3f} = \alpha_1 \alpha_2^{-2} \alpha_3^2 y$. Следовательно, если $f \in R$ и $u_f^{(1)} = \gamma_1 y_k$, где $\gamma_1 \in \Gamma_j$ $(1 \leqslant j \leqslant 2^m)$, то существуют $a_{if}, b_{kf} \in \mathbb{Z}$ $(2 \leqslant i \leqslant p,\ 1 \leqslant k \leqslant p)$, такие что для любого $\gamma \in \Gamma_j$ мы будем иметь $\operatorname{ord}_i u_{\gamma f}^{(i)} = \operatorname{ord} \gamma + a_{if}$ и $\operatorname{ord}_k v_{\gamma f}^{(k)} = \operatorname{ord} \gamma + b_{kf}$.

Предложение 3.7. *Если $f, g \in K\{y_1, \ldots, y_n\}^*$ и $\operatorname{rk} f < \operatorname{rk} g$, то f E-редуцирован относительно g.*

Доказательство. Предположим, что f не является E-редуцированным относительно g. Если f содержит некоторую степень терма вида $\bigl(\gamma u_g^{(1)}\bigr)^e$, где $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$ и $e \geqslant d = \deg_{u_g^{(1)}} g$, то $\gamma = 1$ (если $\gamma \neq 1$, то $u_g^{(1)} <_1 \gamma u_g^{(1)} \leqslant_1 u_f^{(1)}$, что противоречит условию (7) для неравенства $\operatorname{rk} f < \operatorname{rk} g$). Следовательно, так как f не является E-редуцированным относительно g, мы имеем $\operatorname{ord}_k u_g^{(k)} \leqslant \operatorname{ord}_k u_f^{(k)}$ $(k = 2, \ldots, p)$ и $\operatorname{ord}_k v_g^{(k)} \geqslant \operatorname{ord}_k v_f^{(k)}$ $(k = 1, \ldots, p)$. Мы получаем, что $\operatorname{Eord}_k g \leqslant \operatorname{Eord}_k f$ $(1 \leqslant k \leqslant p)$, а это противоречит неравенству $\operatorname{rk} f < \operatorname{rk} g$. Следовательно, σ^*-многочлен f E-редуцирован относительно g. $\square$

Предложение 3.8. *Пусть* $\mathcal{A} = \{g_1, \dots, g_t\}$ *— конечное множество* σ^**-многочленов из кольца* $R = K\{y_1, \dots, y_n\}^*$*. Пусть* $u_k^{(i)}$ *и* $v_k^{(i)}$ *—* i*-лидер и* i*-колидер* σ^**-многочлена* g_k *соответственно,* $1 \leqslant k \leqslant t$*,* $1 \leqslant i \leqslant p$*. Пусть* $d_k = \deg_{u_k^{(1)}} g_k$*, и пусть* I_k *обозначает коэффициент при* $(u_k^{(1)})^{d_k}$*, когда* g_k *записывается как многочлен от одного неизвестного* $u_k^{(1)}$ $(1 \leqslant k \leqslant t)$*. Кроме того, пусть*

$$\begin{aligned} I(\mathcal{A}) = \{f \in R \mid & \text{ либо } f = 1, \text{ либо } f \text{ является произведением} \\ & \text{конечного числа } \sigma^*\text{-многочленов вида } \gamma(I_k),\ \gamma \in \Gamma,\ k = 1, \dots, t\}. \end{aligned}$$

Тогда для любого $h \in R$ *существуют* $J \in I(\mathcal{A})$ *и* $\bar{h} \in R$*, такие что* $\bar{h}$ E*-редуцирован относительно* $\mathcal{A}$ *и* $Jh \equiv \bar{h} \pmod{[\mathcal{A}]^*}$ *(т. е.* $Jh - \bar{h} \in [\mathcal{A}]^*$*).*

Доказательство. Если h E-редуцирован относительно $\mathcal{A}$, наше утверждение очевидно. Допустим, что h не является E-редуцированным относительно $\mathcal{A}$. В дальнейшем, если σ^*-многочлен $f \in R$ не является E-редуцированным относительно $\mathcal{A}$, терм w_f, который входит в f, будем называть *$\mathcal{A}$-лидером* σ^*-многочлена f, если w_f — наибольший (относительно порядка $<_1$) терм среди всех термов вида $\gamma u_{g_k}^{(1)}$, где $\gamma \in \Gamma$, $\gamma \sim u_{g_k}^{(1)}$ $(1 \leqslant k \leqslant t)$, таких что f содержит степень $\bigl(\gamma u_k^{(1)}\bigr)^e$, в которой $e \geqslant d_k$ и при этом $\operatorname{ord}_i u_{\gamma g_k}^{(i)} \leqslant \operatorname{ord}_i u_f^{(i)}$ $(i = 2, \dots, p)$ и $\operatorname{ord}_j v_{\gamma g_k}^{(i)} \geqslant \operatorname{ord}_j v_f^{(j)}$ $(j = 1, \dots, p)$.

Пусть w_h — $\mathcal{A}$-лидер σ^*-многочлена h, $d = \deg_{w_h} h$ и c_h — коэффициент при w_h^d, когда h представлен как многочлен от w_h. Тогда $w_h = \gamma u_k^{(1)}$ для некоторых $k \in \{1, \dots, t\}$ и $\gamma \in \Gamma$, таких что $\gamma \sim u_{g_k}^{(1)}$, $d \geqslant d_k$, $\operatorname{ord}_i u_{\gamma g_k}^{(i)} \leqslant$ $\leqslant \operatorname{ord}_i u_h^{(i)}$ $(2 \leqslant i \leqslant p)$ и $\operatorname{ord}_j v_{\gamma g_k}^{(j)} \geqslant \operatorname{ord}_j v_h^{(j)}$ $(1 \leqslant j \leqslant p)$. Выберем такое k, которое соответствует максимальному (относительно порядка $<_1$) 1-лидеру $u_i^{(1)}$ $(1 \leqslant i \leqslant t)$ и рассмотрим σ^*-многочлен $h' = \gamma(I_k)h - c_h w_h^{d-d_k}(\gamma g_k)$. Ясно, что $\deg_{w_h} h' < \deg_{w_h} h$ и h' не содержит никакого $\mathcal{A}$-лидера $\gamma' u_\nu^{(1)}$ $(\gamma' \in \Gamma$, $1 \leqslant \nu \leqslant t)$, который был бы больше w_h относительно $<_1$ (такой терм не может входить ни в $\gamma(I_k)h$, ни в γg_k, так как $u_{\gamma g_k}^{(1)} = \gamma u_{g_k}^{(1)} = w_h$). Применяя ту же процедуру к h' и продолжая этот процесс, мы получаем σ^*-многочлен $\bar{h} \in R$, который является E-редуцированным относительно $\mathcal{A}$ и удовлетворяет условию $Jh - \bar{h} \in [\mathcal{A}]^*$ для некоторого $J \in I(\mathcal{A})$. $\square$

Процесс редукции, описанный в доказательстве последнего предложения может быть реализован следующим алгоритмом. (Напомним, что $\mathcal{E}_R$ обозначает кольцо σ^*-операторов над σ^*-кольцом $R = K\{y_1, \dots, y_n\}^*$.)

Алгоритм. $(h, t, g_1, \dots, g_t; \bar{h})$.

Дано: $h \in R$, положительное целое t, $\mathcal{A} = \{g_1, \dots, g_t\} \subseteq R$, где $g_i \neq 0$ для $i = 1, \dots, t$

```
Надо: элемент $\bar{h} \in R$, элементы $C_1, \dots, C_t \in \mathcal{E}_R$ и $J \in I(\mathcal{A})$, такие что $Jh = \sum_{i=1}^{t} C_i(g_i) + \bar{h}$ и $\bar{h}$ $E$-редуцирован относительно множества s$\mathcal{A}$
Начало
$C_1 := 0,\ \dots,\ C_t := 0,\ \bar{h} := h$
Пока существует $k$, $1 \leqslant k \leqslant t$, и терм $w$, входящий в $\bar{h}$ с (ненулевым) коэффициентом $c_w$, такие что $u_{g_k}^{(1)} \mid w$, $\deg_{u_{g_k}^{(1)}} g_k \leqslant \deg_w \bar{h}$, $\operatorname{ord}_i\bigl(\gamma_{kw} u_{g_k}^{(i)}\bigr) \leqslant \operatorname{ord}_i u_{\bar{h}}^{(i)}$ $(2 \leqslant i \leqslant p)$, где $\gamma_{kw} = \frac{w}{u_{g_k}^{(1)}}$, и также $\operatorname{ord}_j\bigl(\gamma_{kw} v_{g_k}^{(j)}\bigr) \geqslant \operatorname{ord}_j v_{\bar{h}}^{(j)}$ при $j = 1, \dots, p$, выполнять:
    $z :=$ наибольший из термов $w$, которые удовлетворяют приведённому выше условию
    $l :=$ наименьшее число $k$, для которого $u_{g_k}^{(1)}$ является наибольшим (относительно $<_1$) 1-лидером элемента множества $\mathcal{A}$, удовлетворяющий условиям $u_{g_k}^{(1)} \mid z$, $\deg_{u_{g_k}^{(1)}} g_k \leqslant \deg_z \bar{h}$, $\operatorname{ord}_i\bigl(\gamma_{kz} u_{g_k}^{(i)}\bigr) \leqslant \operatorname{ord}_i u_{\bar{h}}^{(i)}$ $(i = 2, \dots, p)$, где $\gamma_{kz} = \frac{z}{u_{g_k}^{(1)}}$, и $\operatorname{ord}_j\bigl(\gamma_{kz} v_{g_k}^{(j)}\bigr) \geqslant \operatorname{ord}_j v_{\bar{h}}^{(j)}$ $(j = 1, \dots, p)$;
    $J := \gamma(I_l)J$, $C_l := C_l + c_z z^{d-d_l}\gamma_{lz}$, где $d = \deg_z \bar{h}$, $d_l = \deg_{u_{g_l}^{(1)}} g_l$ и $c_z$ является коэффициентом при $z^d$, когда $\bar{h}$ представлен как многочлен от $z$;
    $\bar{h} := \tau(I_l)h^* - c_z z^{d-d_l}(\gamma g_l)$
Конец
```

Определение 3.9. Множество $\mathcal{A} \subseteq K\{y_1, \dots, y_n\}^*$ называется *E-авторедуцированным*, если оно либо пусто, либо $\mathcal{A} \cap K = \varnothing$ и любые два σ^*-многочлена из множества $\mathcal{A}$ E-редуцированы друг относительно друга.

Пример. Пусть K — инверсное разностное поле с базисным множеством $\sigma = \{\alpha_1, \alpha_2\}$, рассматриваемое вместе с его разбиением $\sigma = \sigma_1 \cup \sigma_2$, где $\sigma_1 = \{\alpha_1\}$ и $\sigma_2 = \{\alpha_2\}$. Пусть $\mathcal{A} = \{g, h\} \subseteq K\{y\}^*$ (кольцо σ^*-многочленов от одного σ^*-неизвестного y), где

$$g = \alpha_1^3\alpha_2^{-2}y + \alpha_2^3 y + \alpha_2 y, \quad h = \alpha_1^2\alpha_2^{-1}y + \alpha_1^{-1}\alpha_2^2 y + \alpha_1\alpha_2 y.$$

В этом случае $u_g^{(1)} = \alpha_1^3\alpha_2^{-2}y$, $v_g^{(1)} = u_g^{(2)} = \alpha_2^3 y$, $v_g^{(2)} = \alpha_2 y$, $u_h^{(1)} = \alpha_1^2\alpha_2^{-1}y$, $v_h^{(1)} = v_h^{(2)} = \alpha_1\alpha_2 y$ и $u_h^{(2)} = \alpha_1^{-1}\alpha_2^2 y$. Мы видим, что $u_g^{(1)}$ — трансформа терма $u_h^{(1)}$, $u_g^{(1)} = \gamma u_h^{(1)}$, где $\gamma = \alpha_1\alpha_2^{-1} \sim u_h^{(1)}$. Кроме того, $\gamma h = \alpha_1^3\alpha_2^{-2}y + \alpha_1^2 y + \alpha_2 y$, так что $u_{\gamma h}^{(1)} = u_{\gamma h}^{(2)} = \alpha_1^3\alpha_2^{-2}y$, $v_{\gamma h}^{(1)} = \alpha_2 y$ и $v_{\gamma h}^{(2)} = \alpha_1^2 y$. Таким образом, $\operatorname{ord}_2 u_{\gamma h}^{(2)} = 2 < \operatorname{ord}_2 u_g^{(2)} = 3$, $\operatorname{ord}_1 v_{\gamma h}^{(1)} = 0 = \operatorname{ord}_1 v_g^{(1)}$, но $\operatorname{ord}_2 v_{\gamma h}^{(2)} = 0 < \operatorname{ord}_2 v_g^{(2)} = 1$. Следовательно, g E-редуцирован относительно h. Очевидно, что h E-редуцирован относительно g, поэтому множество $\mathcal{A} = \{g, h\}$ является

E-автоfeдуцированным. В то же время это множество не является авторедуцированным в смысле [14], где аналог определения 3.4 не предусматривает второй части этого определения.

Мы собираемся показать, что каждое E-авторедуцированное множество конечно. Доказательство следующей леммы дано в [4, гл. 0, раздел 17].

Лемма 3.10. *Пусть A — бесконечное подмножество множества $\mathbb{N}^m \times \mathbb{N}_n$ $(m, n \geqslant 1)$. Тогда существует бесконечная последовательность элементов множества A, которая строго возрастает относительно порядка произведения и в которой все элементы имеют одну и ту же проекцию на $\mathbb{N}_n$.*

Так как каждая бесконечная последовательность элементов множества Γ содержит бесконечную подпоследовательность, в которой все элементы подобны друг другу (число ортантов множества $\mathbb{Z}^m$ конечно), из последней леммы немедленно вытекает следующее утверждение.

Лемма 3.11. *Пусть S — произвольное бесконечное множество термов γy_j $(\gamma \in \Gamma,\ 1 \leqslant j \leqslant n)$ в кольце $K\{y_1, \ldots, y_n\}^*$. Тогда существуют индекс j $(1 \leqslant j \leqslant n)$ и бесконечная последовательность термов $\gamma_1 y_j, \gamma_2 y_j, \ldots, \gamma_k y_j, \ldots$ из S, таких что $\gamma_k \mid \gamma_{k+1}$ для всех $k = 1, 2, \ldots$.*

Предложение 3.12. *Каждое E-авторедуцированное множество конечно.*

Доказательство. Допустим, что имеется бесконечное E-авторедуцированное множество $\mathcal{A}$. Из леммы 3.11 следует, что $\mathcal{A}$ содержит последовательность σ^*-многочленов $\{f_1, f_2, \ldots\}$, такую что $u^{(1)}_{f_i} \mid u^{(1)}_{f_{i+1}}$ $(i = 1, 2, \ldots)$. Так как последовательность целых неотрицательных чисел $\bigl\{\deg_{u^{(1)}_{f_i}} f_i\bigr\}$ не может содержать бесконечную убывающую подпоследовательность, без ограничения общности мы можем считать, что $\deg_{u^{(1)}_{f_i}} f_i \leqslant \deg_{u^{(1)}_{f_{i+1}}} f_{i+1}$ $(i = 1, 2, \ldots)$. Пусть $k_{ij} = \operatorname{ord}_j u^{(1)}_{f_i}$, $l_{ij} = \operatorname{ord}_j u^{(j)}_{f_i}$ и $n_{ij} = \operatorname{ord}_j v^{(j)}_{f_i}$ $(1 \leqslant j \leqslant p)$. Ясно, что $l_{ij} \geqslant k_{ij} \geqslant n_{ij}$ $(i = 1, 2, \ldots;\ j = 1, \ldots, p)$, так что

$$\{(l_{i1} - k_{i1} = 0,\ l_{i2} - k_{i2}, \ldots, l_{ip} - k_{ip}) \mid i = 1, 2, \ldots\} \subseteq \mathbb{N}^p$$

и

$$\{(k_{i1} - n_{i1},\ k_{i2} - n_{i2}, \ldots, k_{ip} - n_{ip}) \mid i = 1, 2, \ldots\} \subseteq \mathbb{N}^p.$$

Применяя лемму 3.10, мы получаем, что существует бесконечная последовательность индексов $i_1 < i_2 < \ldots$, такая что

$$(l_{i_1 2} - k_{i_1 2}, \ldots, l_{i_1 p} - k_{i_1 p}) \leqslant_P (l_{i_2 2} - k_{i_2 2}, \ldots, l_{i_2 p} - k_{i_2 p}) \leqslant_P \ldots \tag{8}$$

и

$$(k_{i_1 1} - n_{i_1 1}, \ldots, k_{i_1 p} - n_{i_1 p}) \leqslant_P (k_{i_1 1} - n_{i_1 1}, \ldots, k_{i_2 p} - n_{i_2 p}) \leqslant_P \ldots. \tag{9}$$

Тогда для каждого $j = 2, \ldots, p$ и для $\gamma_{12} = \dfrac{u^{(1)}_{f_{i_2}}}{u^{(1)}_{f_{i_1}}}$ мы получаем (используя (8))

$$\operatorname{ord}_j u^{(j)}_{\gamma_{12} f_{i_1}} \leqslant \operatorname{ord}_j \gamma_{12} u^{(j)}_{f_{i_1}} = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \leqslant k_{i_2 j} + l_{i_2 j} - k_{i_2 j} = l_{i_2 j} = \operatorname{ord}_j u^{(j)}_{f_{i_2}}.$$

Аналогичное рассуждение с использованием (9) показывает, что $\operatorname{ord}_j\bigl(\tau v^{(j)}_{f_{i_1}}\bigr) \geqslant \operatorname{ord}_j v^{(j)}_{f_{i_2}}$ $(j = 2, \ldots, p)$. Таким образом, σ^*-многочлен f_{i_2} не является E-редуцированным относительно f_{i_1}, что противоречит тому, что множество $\mathcal{A}$ является E-автoредуцированным. □

В дальнейшем мы всегда предполагаем, что элементы любого E-авторедуцированного множества расположены в порядке возрастания их рангов.

Определение 3.13. Пусть $\mathcal{A} = \{g_1, \ldots, g_s\}$ и $\mathcal{B} = \{h_1, \ldots, h_t\}$ — два E-авторедуцированных множества в кольце $K\{y_1, \ldots, y_n\}^*$. Мы говорим, что множество $\mathcal{A}$ ниже рангом, чем множество $\mathcal{B}$, и пишем $\operatorname{rk}\mathcal{A} < \operatorname{rk}\mathcal{B}$, если выполняется одно из следующих условий:

1) $\operatorname{rk} g_1 < \operatorname{rk} h_1$ или существует $k \in \mathbb{N}$, такое что $1 < k \leqslant \min\{s, t\}$, $\operatorname{rk} g_i = \operatorname{rk} h_i$ при $i = 1, \ldots, k-1$ и $\operatorname{rk} g_k < \operatorname{rk} h_k$;
2) $s > t$ и $\operatorname{rk} g_i = \operatorname{rk} h_i$ при $i = 1, \ldots, t$.

Если $s = t$ и $\operatorname{rk} g_i = \operatorname{rk} h_i$ при $i = 1, \ldots, s$, мы говорим, что множества $\mathcal{A}$ и $\mathcal{B}$ имеют один и тот же ранг; в этом случае мы пишем $\operatorname{rk}\mathcal{A} = \operatorname{rk}\mathcal{B}$.

Предложение 3.14. *Каждое семейство E-авторедуцированных множеств в кольце σ^*-многочленов $K\{y_1, \ldots, y_n\}^*$ содержит E-авторедуцированное множество наименьшего ранга.*

Доказательство. Мы будем следовать схеме доказательства соответствующего утверждения о дифференциальных многочленах (см. [4, гл. 1, утверждение 3]. Пусть $\mathcal{M}$ — непустое семейство E-авторедуцированных множеств в кольце $K\{y_1, \ldots, y_n\}^*$. Мы построим бесконечную убывающую цепь подмножеств множества $\mathcal{M}$ по индукции: положим

$$\begin{aligned}
&\mathcal{M}_0 = \mathcal{M},\\
&\mathcal{M}_1 = \{\mathcal{A} \in \mathcal{M}_0 \mid \mathcal{A} \text{ содержит хотя бы один элемент и первый элемент}\\
&\qquad\qquad \text{множества } \mathcal{A} \text{ имеет наименьший возможный ранг}\}, \ldots,\\
&\mathcal{M}_k = \{\mathcal{A} \in \mathcal{M}_{k-1} \mid \mathcal{A} \text{ содержит не меньше } k \text{ элементов и } k\text{-й элемент}\\
&\qquad\qquad \text{множества } \mathcal{A} \text{ имеет наименьший возможный ранг}\}, \ldots .
\end{aligned}$$

Ясно, что если $\mathcal{A}$ и $\mathcal{B}$ — два E-авторедуцированных множества в $\mathcal{M}_k$ и если f и g — l-е элементы множеств $\mathcal{A}$ и $\mathcal{B}$ соответственно $(l \geqslant k)$, то $\operatorname{rk} f = \operatorname{rk} g$. Следовательно, если все множества $\mathcal{M}_k$ были бы непусты, то множество

$$\{A_k \mid A_k \text{ — } k\text{-й элемент некоторого } E\text{-авторедуцированного множества из } \mathcal{M}_k\}$$

было бы бесконечным E-авторедуцированным множеством, что противоречит предложению 3.12. Таким образом, существует наименьшее целое положительное число k, такое что $\mathcal{M}_k = \varnothing$. Очевидно, что каждый элемент множества $\mathcal{M}_{k-1}$ является E-авторедуцированным множеством наименьшего ранга в семействе $\mathcal{M}$. □

Пусть J — ненулевой идеал кольца $K\{y_1, \ldots, y_n\}^*$. Так как множество E-авторедуцированных подмножеств идеала J непусто (если $0 \neq f \in J$, то $\{f\}$ — E-авторедуцированное множество), предложение 3.14 показывает, что J содержит E-авторедуцированное множество наименьшего ранга. Это множество называется *E-характеристическим множеством* идеала J.

Предложение 3.15. *Пусть J — идеал кольца σ^*-многочленов $K\{y_1, \ldots, y_n\}^*$ и $\mathcal{A} = \{f_1, \ldots, f_d\}$ — его E-характеристическое множество. Тогда элемент $g \in J$ E-редуцирован относительно $\mathcal{A}$ тогда и только тогда, когда $g = 0$.*

Доказательство. Заметим, что если $g \neq 0$ и $\operatorname{rk} g < \operatorname{rk} f_1$, то $\operatorname{rk}\{g\} < \operatorname{rk} \mathcal{A}$, что противоречит тому, что $\mathcal{A}$ является E-характеристическим множеством идеала J. Пусть $\operatorname{rk} g > \operatorname{rk} f_1$ и $f_1, \ldots, f_j$ $(1 \leqslant j \leqslant d)$ — все элементы множества $\mathcal{A}$, ранг которых ниже ранга g. Тогда множество $\mathcal{A}' = \{f_1, \ldots, f_j, g\}$ является E-авторедуцированным. Действительно, $f_1, \ldots, f_j$ являются E-редуцированными друг относительно друга и σ^*-многочлен g E-редуцирован относительно множества $\{f_1, \ldots, f_j\}$. Кроме того, каждый σ-многочлен f_i $(1 \leqslant i \leqslant j)$ E-редуцирован относительно g, потому что $\operatorname{rk} f_i < \operatorname{rk} g$. Так как $\operatorname{rk} \mathcal{A}' < \operatorname{rk} \mathcal{A}$, $\mathcal{A}$ не является E-характеристическим множеством идеала J, что противоречит условию нашего предложения. Следовательно, $g = 0$. □

Из замечания 3.5 следует, что каждое авторедуцированное (характеристическое) множество идеала J кольца $K\{y_1, \ldots, y_n\}^*$ в смысле [6, определения 3.4.23 и 3.4.31] относительно $<_1$ является E-авторедуцированным (соответственно E-характеристическим) множеством этого идеала. Это позволяет нам применить [6, следствие 6.5.4] и получить следующий результат.

Предложение 3.16. *Пусть $\preceq$ обозначает предпорядок на $K\{y_1, \ldots, y_n\}^*$, такой что $f \preceq g$ тогда и только тогда, когда $u_g^{(1)}$ является трансформой терма $u_f^{(1)}$. Пусть f — линейный σ^*-многочлен из кольца $K\{y_1, \ldots, y_n\}^* \setminus K$. Тогда множество всех минимальных относительно $\preceq$ элементов множества $\{\gamma f \mid \gamma \in \Gamma\}$ образуют E-характеристическое множество σ^*-идеала $[f]^*$.*

4. Новый тип размерностных многочленов от нескольких переменных, связанных с расширениями σ^*-полей

В этой части мы используем свойства E-характеристических множеств для получения результата, который обобщает теорему 2.1 и вводит новый вид размерностных многочленов от нескольких переменных, связанных с конечно порождёнными расширениями инверсных разностных полей. Эти многочлены содержат больше инвариантов соответствующего расширения, чем разностные размерностные многочлены от одной переменной. (Под инвариантом расширения σ^*-поля мы понимаем числовую характеристику этого расширения, которая не зависит от выбора множества σ^*-образующих этого расширения.) Как прежде, K обозначает инверсное разностное поле (σ^*-поле) с базисным множеством $\sigma = \{\alpha_1, \dots, \alpha_m\}$ и его фиксированным разбиением (6) на p попарно непересекающихся подмножеств σ_i, $\operatorname{Card} \sigma_i = m_i$ $(1 \leqslant i \leqslant p)$. Кроме того, для любых двух p-мерных точек $(r_1, \dots, r_p)$, $(s_1, \dots, s_p) \in \mathbb{N}^p$, таких что $s_i \leqslant r_i$ $(i = 1, \dots, p)$, мы полагаем

$$\Gamma(r_1, \dots, r_p; s_1, \dots, s_p) = \{\gamma \in \Gamma \mid s_i \leqslant \operatorname{ord}_i \gamma \leqslant r_i \text{ для } i = 1, \dots, p\}.$$

Теорема 4.1. *Пусть* $L = K\langle \eta_1, \dots, \eta_n \rangle^*$ *— расширение* σ^**-поля* K*, порождённое множеством* $\eta = \{\eta_1, \dots, \eta_n\}$*. Тогда существуют многочлен* $\Phi_{\eta|K}(t_1, \dots, t_{2p})$ *от* $2p$ *переменных с рациональными коэффициентами и числа* $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leqslant i \leqslant p)$*, такие что* $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ *для любого* i *и*

$$\begin{aligned}\Phi_{\eta|K}(r_1, \dots, r_p, s_1, \dots, s_p) &= \\ &= \operatorname{tr.deg}_K K(\{\gamma\eta_j \mid \gamma \in \Gamma(r_1, \dots, r_p; s_1, \dots, s_p),\ 1 \leqslant j \leqslant n\})\end{aligned}$$

для всех $(r_1, \dots, r_p, s_1, \dots, s_p) \in \mathbb{N}^{2p}$*, таких что* $r_i \geqslant r_i^{(0)}$*,* $s_i^{(1)} \leqslant s_i \leqslant r_i - s_i^{(0)}$*. Кроме того,* $\deg \Phi_{\eta|K} \leqslant m$*,* $\deg_{t_i} \Phi_{\eta|K} \leqslant m_i$ *при* $i = 1, \dots, p$ *и* $\deg_{t_j} \Phi_{\eta|K} \leqslant m_{j-p}$ *при* $j = p + 1, \dots, 2p$*.*

Доказательство. Пусть $P \subseteq R = K\{y_1, \dots, y_n\}$ — определяющий σ^*-идеал расширения L/K, и пусть $\mathcal{A} = \{f_1, \dots, f_q\}$ — E-характеристическое множество идеала P. Для каждых точек $\bar{r} = (r_1, \dots, r_p)$, $\bar{s} = (s_1, \dots, s_p) \in \mathbb{N}^p$, таких что $\bar{s} \leqslant_P \bar{r}$ (т. е. $s_i \leqslant r_i$ для $i = 1, \dots, p$), пусть

$$\begin{aligned}
&W(\bar{r}, \bar{s}) = \{w \in \Gamma Y \mid s_i \leqslant \operatorname{ord}_i w \leqslant r_i \text{ for } i = 1, \dots, p\},\\
&W_\eta(\bar{r}, \bar{s}) = \{w(\eta) \mid w \in W(\bar{r}, \bar{s})\},\\
&U'(\bar{r}, \bar{s}) = \{u \in \Gamma Y \mid s_i \leqslant \operatorname{ord}_i u \leqslant r_i \text{ для } i = 1, \dots, p\\
&\qquad \text{и } u \text{ не является трансформой ни одного терма } u_{f_j}^{(1)},\ 1 \leqslant j \leqslant q\},\\
&U'_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U'(\bar{r}, \bar{s})\},\\
&U''(\bar{r}, \bar{s}) = \{u \in \Gamma Y \mid s_i \leqslant \operatorname{ord}_i u \leqslant r_i,\ 1 \leqslant i \leqslant p,\\
&\qquad u \text{ является трансформой некоторого терма } u_{f_j}^{(1)}, 1 \leqslant j \leqslant q,\\
&\qquad \text{и как только } u = \gamma u_{f_j}^{(1)}\ (\gamma \in \Gamma,\ \gamma \sim u_{f_j}^{(1)}), \text{ то либо } \operatorname{ord}_1 v_{\gamma f_j}^{(1)} < s_1,\\
&\qquad \text{либо существует } k \in \{2, \dots, p\}, \text{ такое что } \operatorname{ord}_k(u_{\gamma f_j}^{(k)}) > r_k,\\
&\qquad \text{либо существует } i \in \{2, \dots, p\}, \text{ такое что } \operatorname{ord}_i v_{\gamma f_j}^{(i)} < s_i\\
&\qquad \text{(«либо» не является исключающим,}\\
&\qquad \text{т. е. возможно выполнение этих условий одновременно)}\},\\
&U''_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U''(\bar{r}, \bar{s})\}.
\end{aligned}$$

Кроме того, пусть

$$U(\bar{r}, \bar{s}) = U'(\bar{r}, \bar{s}) \cup U''(\bar{r}, \bar{s}) \quad \text{и} \quad U_\eta(\bar{r}, \bar{s}) = U'_\eta(\bar{r}, \bar{s}) \cup U''_\eta(\bar{r}, \bar{s}).$$

Мы собираемся доказать, что для любых $\bar{r}, \bar{s} \in \mathbb{N}^p$, таких что $\bar{s} <_P \bar{r}$, множество $U_\eta(\bar{r}, \bar{s})$ является базисом трансцендентности поля $K\bigl(W_\eta(\bar{r}, \bar{s})\bigr)$ над K.

Покажем сначала, что это множество алгебраически независимо над K. Допустим, что $f\bigl(w_1(\eta), \dots, w_k(\eta)\bigr) = 0$ для некоторых элементов $w_1, \dots, w_k \in \in U(\bar{r}, \bar{s})$. Тогда σ^*-многочлен $f(w_1, \dots, w_k)$ должен лежать в P, и этот σ^*-многочлен E-редуцирован относительно $\mathcal{A}$. (Если f содержит терм $w = \gamma u_{f_j}^{(1)}$ $(1 \leqslant i \leqslant q,\ \gamma \in \Gamma,\ \gamma \sim u_{f_j}^{(1)})$, такой что $\deg_w f \geqslant \deg_{u_{f_j}^{(1)}} f_j$, то $w \in U''(\bar{r}, \bar{s})$, так что либо $\operatorname{ord}_1(v_{\gamma f_j}^{(1)}) < s_1 \leqslant \operatorname{ord}_1 v_f^{(1)}$, либо существует $k \in \{2, \dots, q\}$, такое что $\operatorname{ord}_k u_{\gamma f_j}^{(k)} > r_k \geqslant \operatorname{ord}_k u_f^{(k)}$, либо существует $i \in \{2, \dots, p\}$, такое что $\operatorname{ord}_i v_{\gamma f_j}^{(i)} < s_i \leqslant \operatorname{ord}_i v_f^{(i)}$ («либо» не является исключающим). Следовательно, f E-редуцирован относительно $\mathcal{A}$.) По предложению 3.15 $f = 0$, так что множество $U_\eta(\bar{r}, \bar{s})$ алгебраически независимо над K.

Теперь мы покажем, что если $0 \leqslant s_i \leqslant r_i - s_i^{(0)}$, где $s_i^{(0)} = \max\{\operatorname{Eord}_i f_j \mid 1 \leqslant j \leqslant q\}$ $(1 \leqslant i \leqslant p)$, то каждый элемент $\gamma\eta_k \in W_\eta(\bar{r}, \bar{s}) \setminus U_\eta(\bar{r}, \bar{s})$ $(\gamma \in \Gamma,\ 1 \leqslant k \leqslant n)$ алгебраичен над полем $K\bigl(U_\eta(\bar{r}, \bar{s})\bigr)$. В этом случае, так как $\gamma y_k \notin U(\bar{r}, \bar{s})$, γy_k равен некоторому элементу вида $\gamma' u_{f_j}^{(1)}$ $(1 \leqslant j \leqslant q)$, где $\gamma' \in \Gamma$, $\gamma' \sim \gamma' u_j^{(1)}$, $\operatorname{ord}_i u_{\gamma' f_j}^{(i)} \leqslant r_i$ $(i = 2, \dots, p)$ и $\operatorname{ord}_l v_{\gamma' f_j}^{l} \geqslant s_l$ $(l = 1, \dots, p)$.

Представим f_j как многочлен от $u_{f_j}^{(1)}$:

$$f_j = I_{d_j}^{(j)}\bigl(u_{f_j}^{(1)}\bigr)^{d_j} + \ldots + I_1^{(j)} u_{f_j}^{(1)} + I_0^{(j)},$$

где $I_0^{(j)}, I_1^{(j)}, \dots I_{d_j}^{(j)}$ не содержат $u_{f_j}^{(1)}$ (следовательно, все термы этого σ^*-многочлена меньше, чем $u_{f_j}^{(1)}$, относительно порядка $<_1$). Так как $f_j \in P$, $f_j(\eta) = 0$, т. е.

$$I_{d_j}^{(j)}(\eta)\bigl(u_{f_j}^{(1)}(\eta)\bigr)^{d_j} + \ldots + I_1^{(j)}(\eta) u_{f_j}^{(1)}(\eta) + I_0^{(j)}(\eta) = 0. \tag{10}$$

Заметим, что $I_{d_j}^{(j)}(\eta) \neq 0$. Действительно, так как $\operatorname{rk} I_{d_j}^{(j)} < \operatorname{rk} f_j$, равенство $I_{d_j}^{(j)}(\eta) = 0$ означало бы, что $I_{d_j}^{(j)} \in P$. В этом случае множество всех σ^*-многочленов f_l, для которых $\operatorname{rk} f_l < \operatorname{rk} I_{d_j}^{(j)}$, и $I_{d_j}^{(j)}$ образовывали бы E-автоwebsite-редуцированное множество идеала P, ранг которого был бы ниже, чем ранг множества $\mathcal{A}$. Это противоречило бы тому, что $\mathcal{A}$ — E-характеристическое множество идеала P. Аналогичным образом мы можем заключить, что $I_\nu^{(j)} \notin P$ для всех $\nu = 0, \dots, d_j$ (и для всех $j = 1, \dots, q$). Так как P — σ^*-идеал, мы также видим, что $\gamma(I_\nu^{(j)}) \notin P$ для любых $I_\nu^{(j)}$, $\gamma \in \Gamma$. Следовательно, если мы применим отображение γ' к обеим частям равенства (10), то получившееся равенство покажет, что элемент $\gamma' u_{f_j}^{(1)}(\eta) = \gamma\eta_k$ алгебраичен над полем

$$K\bigl(\bigl\{\tilde{\gamma}\eta_l \mid s_i \leqslant \operatorname{ord}_i \tilde{\gamma} \leqslant r_i,\ 1 \leqslant i \leqslant p,\ \tilde{\gamma} y_l <_1 \gamma' u_{f_j}^{(1)}\bigr\}\bigr).$$

(Заметим, что если $I = I_{\nu}^{(j)}$ для некоторых $j \in \{1, \dots, q\}$ и $\nu \in \{0, \dots, d_j\}$, то $\operatorname{ord}_i\bigl(\gamma' u_I^{(i)}\bigr) \leqslant \operatorname{ord}_i u_{\gamma' I}^{(i)} \leqslant r_i$ $(2 \leqslant i \leqslant p)$ и $\operatorname{ord}_k\bigl(\gamma' v_I^{(k)}\bigr) \geqslant \operatorname{ord}_k v_{\gamma' I}^{(k)} \leqslant s_k$ $(1 \leqslant k \leqslant p)$.) Применяя индукцию по вполне упорядоченному (относительно порядка $<_1$) множеству термов ΓY, мы получаем, что множество $U_{\eta}(\bar{r}, \bar{s})$ — базис трансцендентности поля $K(W_{\eta}(\bar{r}, \bar{s})$ над K.

Для того чтобы определить число элементов множества $U_{\eta}(\bar{r}, \bar{s})$, мы оценим размеры множеств $U'_{\eta}(\bar{r}, \bar{s})$ и $U''_{\eta}(\bar{r}, \bar{s})$, т. е. размеры множеств $U'(\bar{r}, \bar{s})$ и $U''(\bar{r}, \bar{s})$. Для каждого $k = 1, \dots, n$, пусть

$$\begin{aligned} A_k = \{(i_1, \dots, i_m) \in \mathbb{Z}^m \mid \\ \alpha_1^{i_1} \dots \alpha_m^{i_m} y_k - 1\text{-лидер некоторого элемента множества } \mathcal{A}\}. \end{aligned}$$

По теореме 2.8 существует целозначный многочлен $\omega_k(t_1, \dots, t_p) \in \mathbb{Q}[t_1, \dots, t_p]$, такой что $\omega_k(r_1, \dots, r_p) = \operatorname{Card} W_{A_k}(r_1, \dots, r_p)$ для всех достаточно больших $(r_1, \dots, r_p) \in \mathbb{N}^p$. Следовательно, если мы положим

$$\psi_{\eta|K}(t_1, \dots, t_p) = \sum_{k=1}^{n} \omega_k(t_1, \dots, t_p),$$

то найдутся числа $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leqslant i \leqslant p)$, удовлетворяющие условию $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$, такие что для всех $\bar{r} = (r_1, \dots, r_p)$, $\bar{s} = (s_1, \dots, s_p) \in \mathbb{N}^p$ с условиями $r_i \geqslant r_i^{(0)}$, $s_i^{(1)} \leqslant s_i \leqslant r_i - s_i^{(0)}$, мы будем иметь

$$\operatorname{Card} U_{\eta}(\bar{r}, \bar{s}) = \psi_{\eta|K}(r_1, \dots, r_p) - \psi_{\eta|K}(s_1 - 1, \dots, s_p - 1). \tag{11}$$

Кроме того, $\deg \psi_{\eta|K} \leqslant m$ и $\deg \psi_{\eta|K} = m$ тогда и только тогда, когда одно из множеств A_k $(1 \leqslant k \leqslant n)$ пусто.

Чтобы оценить число элементов множества $\operatorname{Card} U''(\bar{r}, \bar{s})$, заметим, что это множество состоит из всех термов $\gamma u_{f_j}^{(1)}$ $(\gamma \in \Gamma,\ \gamma \sim u_{f_j}^{(1)},\ 1 \leqslant j \leqslant q)$, таких что $s_i \leqslant \operatorname{ord}_i u_{\gamma f_j}^{(1)} \leqslant r_i$ и либо $\operatorname{ord}_1 v_{\gamma f_j}^{(1)} < s_1$, либо существует $k \in \{2, \dots, p\}$, такое что $\operatorname{ord}_k u_{\gamma f_j}^{(k)} > r_k$, либо существует $i \in \{2, \dots, p\}$, такое что $\operatorname{ord}_i v_{\gamma f_j}^{(i)} < s_i$ (эти случаи не являются взаимоисключающими). Из замечаний 3.6 и 2.10 следует, что если мы зафиксируем j, то число таких термов $\gamma u_{f_j}^{(1)}$, удовлетворяющих условиям $\operatorname{ord}_i v_{\gamma f_j}^{(i)}) = \operatorname{ord} \gamma + b_{i f_j} < s_i$, $\operatorname{ord}_i\bigl(\gamma u_{f_j}^{(1)}\bigr) = \operatorname{ord}_i \gamma + a_{1 f_j} \geqslant s_i$ при $i \in \{k_1, \dots, k_d\} \subseteq \{1, \dots, p\}$, $\operatorname{ord}_i\bigl(v_{\gamma f_j}^{(i)}\bigr) = \operatorname{ord} \gamma + b_{i f_j} \geqslant s_i$ при $i \in \{1, \dots, p\}$, $i \neq k_{\nu}$ $(1 \leqslant \nu \leqslant d)$ и $\operatorname{ord}_i u_{\gamma f_j}^{(i)} = \operatorname{ord} \gamma + a_{i f_j} \leqslant r_i$ при $i = 1, \dots, p$, равно

$$\prod_{\substack{1 \leqslant i \leqslant p, \\ i \neq k_1, \dots, k_d}} \left[\sum_{\mu=0}^{m_i} (-1)^{m_i - \mu} 2^{\mu} \binom{m_i}{\mu} \left(\binom{r_i - a_{i f_j} + \mu}{\mu} - \binom{s_i - b_{i f_j} + \mu - 1}{\mu} \right) \right] \times$$

$$\times \prod_{\nu=1}^{d}\Bigg[\sum_{\mu=0}^{m_{k_\nu}}(-1)^{m_{k_\nu}-\mu}2^{\mu}\binom{m_{k_\nu}}{\mu}\times$$
$$\times\left(\binom{s_{k_\nu}-b_{k_\nu f_j}-1+m_{k_\nu}}{m_{k_\nu}}-\binom{s_{k_\nu}-a_{1f_j}-1+m_{k_\nu}}{m_{k_\nu}}\right)\Bigg] \qquad (12)$$

и аналогичная формула описывает число термов, удовлетворяющих условиям $\operatorname{ord}_i u^{(i)}_{\gamma f_j} > r_i$ при $i \in \{l_1, \ldots, l_e\} \subseteq \{2, \ldots, p\}$ ($\gamma \in \Gamma$, $\gamma \sim u^{(1)}_{f_j}$), $\operatorname{ord}_i v^{(i)}_{\gamma f_j} \geqslant s_i$ при $i \in \{1, \ldots, p\}$ и $\operatorname{ord}_i u^{(i)}_{\gamma f_j} \leqslant r_i$ при $i \neq l_\nu$ ($1 \leqslant \nu \leqslant e$).

Применяя комбинаторный принцип включения и исключения (учитывая термы, которые являются трансформами нескольких 1-лидеров), мы получаем, что $\operatorname{Card} U''(\bar r, \bar s)$ выражается альтернированной суммой многочленов от $r_1, \ldots, r_p$, $s_1, \ldots, s_p$, каждый из которых является произведением k ($0 \leqslant k \leqslant p$) термов вида $\binom{r_i-a_i+m_i}{m_i} - \binom{s_i-b_i+m_i}{m_i}$, где $a_i, b_i \in \mathbb{N}$ ($1 \leqslant i < p$), и $p-k$ термов вида либо $\binom{s_i-c_i+m_i}{m_i} - \binom{s_i-d_i+m_i}{m_i}$, либо $\binom{r_i-c_i+m_i}{m_i} - \binom{r_i-d_i+m_i}{m_i}$, где $c_i, d_i \in \mathbb{N}$, $c_i < d_i$. Так как полная степень каждого такого многочлена не превосходит $m-1$ и его степени относительно r_i или s_i ($1 \leqslant i \leqslant p$) не превосходят m_i, мы получаем, что $\operatorname{Card} U''(\bar r, \bar s) = \lambda(r_1, \ldots, r_p, s_1, \ldots, s_p)$, где $\lambda(t_1, \ldots, t_{2p})$ — целозначный многочлен от $2p$ переменных, такой что $\deg \lambda < m$ и $\deg_{t_i} \lambda \leqslant m_i$, $\deg_{t_j} \lambda \leqslant m_{j-p}$ при $i = 1, \ldots, p$, $j = p+1, \ldots, 2p$. Отсюда следует, что целозначный многочлен

$$\Phi_{\eta|K}(t_1, \ldots, t_{2p}) = \psi_{\eta|K}(t_1, \ldots, t_p) - \psi_{\eta|K}(t_{p+1}-1, \ldots, t_{2p}-1) + \lambda(t_1, \ldots, t_{2p})$$

удовлетворяет условиям нашей теоремы. □

Определение 4.2. Целозначный многочлен $\Phi_{\eta|K}(t_1, \ldots, t_{2p})$, существование которого устанавливает теорема 4.1, называется σ^*-размерностным многочленом от $2p$ переменных, связанным с расширением L/K, системой его σ^*-образующих η и разбиением (6) множества σ.

Следующая теорема даёт некоторые инварианты вводимого теоремой 4.1 размерностного многочлена, т. е. числовых характеристики расширения, которые не зависят от системы его σ^*-образующих (как и прежде, мы фиксируем разбиение (6) множества σ. Мы будем использовать следующие обозначения: для любой перестановки $(j_1, \ldots, j_{2p})$ множества $\{1, \ldots, 2p\}$, $<_{j_1,\ldots,j_{2p}}$ будет обозначать лексикографический порядок на множестве $\mathbb{N}^{2p}$, такой что $(k_1, \ldots, k_{2p}) <_{j_1,\ldots,j_{2p}} (l_1, \ldots, l_{2p})$ тогда и только тогда, когда либо $k_{j_1} < l_{j_1}$, либо существует $q \in \mathbb{N}$, $2 \leqslant q \leqslant 2p$, такое что $k_{j_\nu} = l_{j_\nu}$ при $\nu < q$ и $k_{j_q} < l_{j_q}$.

Теорема 4.3. *Пусть $\Phi_{\eta|K}(t_1, \ldots, t_{2p})$ — σ^*-размерностный многочлен от $2p$ переменных расширения $L = K\langle\eta_1, \ldots, \eta_n\rangle^*$, связанный с семейством $\eta = \{\eta_1, \ldots, \eta_n\}$ σ^*-образующих этого расширения. Так как степени многочлена $\Phi_{\eta|K}$ относительно t_i и t_{p+i} ($1 \leqslant i \leqslant p$) не превосходят $m_i = \operatorname{Card}\sigma_i$ (см. разбиение (6)), теорема 2.3 показывает, что этот многочлен представим в виде*

$$\Phi_{\eta|K} = \sum_{i_1=0}^{m_1}\cdots\sum_{i_p=0}^{m_p}\sum_{i_{p+1}=0}^{m_1}\cdots\sum_{i_{2p}=0}^{m_p} a_{i_1\ldots i_{2p}}\binom{t_1+i_1}{i_1}\cdots\binom{t_{2p}+i_{2p}}{i_{2p}}.$$

Пусть

$$E_\eta = \{(i_1, \dots, i_{2p}) \in \mathbb{N}^{2p} \mid 0 \leqslant i_k, i_{p+k} \leqslant m_k, k = 1, \dots, p, \text{ и } a_{i_1 \dots i_{2p}} \neq 0\}.$$

Тогда полная степень d многочлена $\Phi_{\eta|K}$ относительно переменных $t_1, \dots, t_p$ и коэффициенты при мономах полной степени d этого многочлена не зависят от системы σ^*-образующих η. Кроме того, если $(\mu_1, \dots, \mu_p)$ — любая перестановка множества $\{1, \dots, p\}$ и $(\nu_1, \dots, \nu_p)$ — любая перестановка множества $\{p+1, \dots, 2p\}$, то максимальный элемент множества E_η относительно порядка $<_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ и соответствующий коэффициент $a_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ также не зависят от системы σ^*-образующих расширения L/K. Наконец, $a_{m_1 \dots m_p 0 \dots 0} = a_{0 \dots 0 m_1 \dots m_p} = \sigma\text{-}\operatorname{tr.deg}_K L$.

Доказательство. Пусть $\zeta = \{\zeta_1, \dots, \zeta_l\}$ — другая система σ^*-образующих L/K, т. е. $L = K\langle \eta_1, \dots, \eta_n \rangle^* = K\langle \zeta_1, \dots, \zeta_l \rangle^*$. Пусть

$$\Phi_{\zeta|K}(t_1, \dots, t_{2q}) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} \sum_{i_{p+1}=0}^{m_1} \dots \sum_{i_{2p}=0}^{m_p} b_{i_1 \dots i_{2p}} \binom{t_1 + i_1}{i_1} \dots \binom{t_{2p} + i_{2p}}{i_{2p}} -$$

σ^*-размерностный многочлен от $2p$ переменных расширения L/K, связанный с системой его σ^*-образующих ζ. Тогда существуют $h_1, \dots, h_p \in \mathbb{N}$, такие что

$$\eta_i \in K\biggl(\bigcup_{j=1}^{l} \Gamma(h_1, \dots, h_p)\zeta_j\biggr) \quad \text{и} \quad \zeta_k \in K\biggl(\bigcup_{j=1}^{n} \Gamma(h_1, \dots, h_p)\eta_j\biggr)$$

для любых $i = 1, \dots, n$ и $k = 1, \dots, l$. (Если $\Gamma' \subseteq \Gamma$, то $\Gamma'\zeta_j$ обозначает множество $\{\gamma\zeta_j \mid \gamma \in \Gamma'\}$.) Следовательно, существуют $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leqslant i \leqslant p)$, такие что $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ и как только $r_i \geqslant r_i^{(0)}$, $s_i^{(1)} \leqslant s_i \leqslant r_i - s_i^{(0)}$ $(1 \leqslant i \leqslant p)$, имеют место неравенства

$$\Phi_{\eta|K}(r_1, \dots, r_{2p}) \leqslant \Phi_{\zeta|K}(r_1 + h_1, \dots, r_p + h_p, r_{p+1} - h_1, \dots, r_{2p} - h_p)$$

и

$$\Phi_{\zeta|K}(r_1, \dots, r_{2p}) \leqslant \Phi_{\zeta|K}(r_1 + h_1, \dots, r_p + h_p, r_{p+1} - h_1, \dots, r_{2p} - h_p).$$

Теперь утверждение нашей теоремы о максимальных элементах множества E_η относительно лексикографических порядков $<_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ и соответствующих коэффициентах следует из того, что для любого $(k_1, \dots, k_{2p}) \in E'_\eta$ терм $\binom{t_1+k_1}{k_1} \dots \binom{t_{2p}+k_{2p}}{k_{2p}}$ входит в $\Phi_{\eta|K}(t_1, \dots, t_{2p})$ и $\Phi_{\zeta|K}(t_1, \dots, t_{2p})$ с одним и тем же коэффициентом $a_{k_1 \dots k_{2p}}$. Равенство коэффициентов при соответствующих членах полной степени $d = \deg \Phi_{\eta|K} = \deg \Phi_{\zeta|K}$ в многочленах $\Phi_{\eta|K}$ и $\Phi_{\zeta|K}$ следует из рассуждений, подобных применённым при доказательстве теоремы 3.3.21 в [12].

Чтобы доказать последнюю часть теоремы, заметим, что выражение (12) и аналогичное выражение, соответствующее условиям $\operatorname{ord}_i u_{\gamma f_j}^{(i)} > r_i$ при $i \in \{l_1, \dots, l_e\} \subseteq \{2, \dots, p\}$ $(\gamma \in \Gamma,\ \gamma \sim u_{f_j}^{(1)})$, $\operatorname{ord}_i v_{\gamma f_j}^{(i)} \geqslant s_i$ при $i \in \{1, \dots, p\}$

и $\operatorname{ord}_i u^{(i)}_{\gamma f_j} \leqslant r_i$ при $i \neq l_\nu$, где $\nu = 1, \ldots, e$ (см. доказательство теоремы 4.1), таковы, что их полные степени относительно $r_1, \ldots, r_p$ и относительно $s_1, \ldots, s_p$ меньше, чем m. Отсюда следует, что коэффициенты при мономах полной степени m относительно $t_1, \ldots, t_p$ и мономах полной степени m относительно $t_{p+1}, \ldots, t_{2p}$ в многочлене $\Phi_{\eta|K}$ равны соответствующим коэффициентам в многочленах $\psi_{\eta|K}(t_1, \ldots, t_p)$ и $\psi_{\eta|K}(t_{p+1}, \ldots, t_{2p})$ соответственно (см. (11)). Теперь, используя тот факт, что если элементы $\eta_{i_1}, \ldots, \eta_{i_k}$ $(i_1, \ldots, i_k \in \{1, \ldots, n\})$ σ-алгебраически независимы над K, то

$$\begin{aligned}\operatorname{tr.deg}_K K(\{\gamma\eta_{i_j} \mid \gamma \in \Gamma(r_1, \ldots, r_p; s_1, \ldots, s_p),\ 1 \leqslant j \leqslant k\}) &= \\ = k\prod_{i=1}^{p}\Bigg[\sum_{j=0}^{m_i}(-1)^{m_i-j}2^j\binom{m_i}{j}\bigg(\binom{r_i+j}{j} - \binom{s_i+j-1}{j}\bigg)\Bigg]\end{aligned}$$

для любых $r_i, s_i \in \mathbb{N}$, таких что $s_i \leqslant r_i$ $(1 \leqslant i \leqslant p)$, мы можем повторить доказательство теоремы 6.4.8 из [6] и получить, что $a_{m_1 \ldots m_p 0 \ldots 0} = a_{0 \ldots 0 m_1 \ldots m_p} = \sigma\text{-}\operatorname{tr.deg}_K L$. □

Пример. Пусть K — инверсное разностное поле (σ^*-поле) с базисным множеством $\sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ и фиксировано разбиение $\sigma = \{\alpha_1\} \cup \{\alpha_2\} \cup \{\alpha_3\}$. Пусть $L = K\langle\eta\rangle^*$ — расширение σ^*-поля с определяющим уравнением

$$\alpha_1^a\eta + \alpha_1^{-a}\eta + \alpha_2^b\eta + \alpha_3^c\eta = 0, \tag{13}$$

где $a, b, c \in \mathbb{N}$, $a > b > c > 0$. Это означает, что определяющий σ^*-идеал P расширения L/K — линейный σ^*-идеал кольца σ^*-многочленов $K\{y\}^*$, порождённый σ^*-многочленом $f = \alpha_1^a y + \alpha_1^{-a} y + \alpha_2^b y + \alpha_3^c y$.

По предложению 3.16 σ^*-многочлены f и

$$\alpha_1^{-1} f = \alpha_1^{-(a+1)} y + \alpha_1^{a-1} y + \alpha_1^{-1}\alpha_2^b y + \alpha_1^{-1}\alpha_3^c y$$

образуют E-характеристическое множество идеала P. Полагая $\bar{r} = (r_1, r_2, r_3)$, $\bar{s} = (s_1, s_2, s_3)$ и используя обозначения из доказательства теоремы 4.1, мы получаем (применяя теоремы 2.6 и 2.8), что

$$\begin{aligned}\operatorname{Card} U'_\eta(\bar{r}, \bar{s}) = \varphi_{\{(a,0,0),(-a-1,0,0)\}}(r_1, r_2, r_3, s_1, s_2, s_3) &= \\ = 2a(2r_2 - 2s_2 + 2)(2r_3 - 2s_3 + 2)\end{aligned}$$

для всех достаточно больших $(r_1, r_2, r_3, s_1, s_2, s_3) \in \mathbb{N}^6$. Кроме того, используя комбинаторный метод включения и исключения (как указано в доказательстве теоремы 4.1), мы получаем

$$\begin{aligned}\operatorname{Card} U''_\eta(\bar{r}, \bar{s}) &= (2a+1)(2r_2 - 2s_2 + 2)(2r_3 - 2s_3 + 2) + \\ &+ 4b(r_1 - s_1 + 1)(2r_3 - 2s_3 + 2) + 4c(r_1 - s_1 + 1)(2r_2 - 2s_2 + 2) - \\ &- 2b(2a+1)(2r_3 - 2s_3 + 2) - 2c(2a+1)(2r_2 - 2s_2 + 2) - \\ &- 8bc(r_1 - s_1 + 1) + 8abc + 4bc.\end{aligned}$$

Так как σ^*-размерностный многочлен от шести переменных $\Phi_{\eta|K}$ выражает число элементов множества $U'_\eta(\bar{r},\bar{s}) \cup \operatorname{Card} U''_\eta(\bar{r},\bar{s})$ для всех достаточно больших значений его аргументов, мы получаем, что

$$\begin{aligned}\Phi_{\eta|K}(t_1,\ldots,t_6) &= 8ct_1t_2 + 8bt_1t_3 - 8ct_1t_5 - 8bt_1t_6 + \\ &+ 4(4a+1)t_2t_3 - 8ct_2t_4 - 4(4a+1)t_2t_6 - 8bt_3t_4 - \\ &- 4(4a+1)t_3t_5 + 8ct_4t_5 + 8bt_4t_6 + 4(4a+1)t_5t_6 + \\ &+ \text{линейная комбинация мономов степени не выше } 1. \end{aligned} \tag{14}$$

σ^*-размерностный многочлен от одной переменной $\varphi_{\eta|K}(t)$ (см. теорему 2.1) имеет следующий вид (по [6, теорема 6.4.8] он совпадает с размерностным многочленом, связанным с подмножеством $A = \{(a,0,0),\ (-a-1,0,0)\}$ множества $\mathbb{Z}^3$ в случае $p=1$, так что его можно вычислить с помощью теорем 2.8 и 2.6):

$$\varphi_{\eta|K}(t) = 4at^2 + \text{линейная комбинация мономов степени не выше } 1.$$

По теореме 4.3 $\deg \Phi_{\eta|K} = 2$ и коэффициенты при мономах t_it_j $(1 \leqslant i,j \leqslant 6)$ являются инвариантами расширения L/K, т. е. они не зависят от множества σ^*-образующих этого расширения. Следовательно, многочлен $\Phi_{\eta|K}(t_1,\ldots,t_6)$ даёт все три параметра a, b и c определяющего уравнения (13), в то время как многочлен $\varphi_{\eta|K}(t)$ несёт в себе только один параметр a.

Тот факт, что σ^*-размерностный многочлен от $2p$ переменных несёт больше инвариантов соответствующего расширения, чем σ^*-размерностный многочлен от одного переменного, может быть полезен при решении задачи об эквивалентности двух систем алгебраических разностных уравнений. Допустим, что у нас есть две системы таких уравнений над σ^*-полем K (т. е. две системы уравнений вида $f_i = 0$ $(i \in I)$, где f_i лежат в некотором кольце σ^*-многочленов $K\{y_1,\ldots,y_n\}^*)$, которые являются определяющими системами уравнений конечно порождённых расширений σ^*-полей L/K и L'/K. (Это значит, что левые части этих систем порождают простые σ^*-идеалы P и P' соответствующих колец σ^*-многочленов R и R' (возможно, от разного числа σ^*-неизвестных), такие что L и L' σ-изоморфны σ^*-полям частных фактор-колец R/P и R'/P' соответственно). Такие две системы называются *эквивалентными*, если существует σ-изоморфизм поля L на L', тождественный на K.

σ^*-размерностный многочлен от $2p$ переменных, введённый в теореме 4.1, позволяет определить, что две системы алгебраических разностных уравнений не являются эквивалентными, в случае когда соответствующие расширения σ^*-полей имеют одни и те же инварианты, которые дают их σ^*-размерностные многочлены от одной переменной. В качестве примера рассмотрим разностные уравнения

$$\alpha_1^a\eta + \alpha_1^{-a}\eta + \alpha_2^b\eta + \alpha_3^c\eta = 0 \tag{15}$$

и

$$\alpha_1^a\eta + \alpha_1^{-a}\eta + \alpha_2^d\eta + \alpha_3^e\eta = 0, \tag{16}$$

где $a,b,c,d,e \in \mathbb{N}$, $a > b > c > 0$ and $a > d > e > 0$. Инварианты, даваемые σ^*-размерностными многочленами от одной переменной, связанными с этими уравнениями (уравнение (15) рассматривалось в последнем примере), одинаковы: степень, равная 1, и параметр a. В то же время σ^*-размерностные многочлены от шести переменных, связанные с этими уравнениями, несут в себе параметры a, b, c и d, e, c соответственно (эти многочлены имеют вид (14)). Таким образом, если, скажем, $d \neq b$, то разностные уравнения (15) и (16) не эквивалентны, несмотря на то что инварианты, даваемые их σ^*-размерностными многочленами от одной переменной, совпадают.

Эта работа была выполнена при поддержке гранта Национального научного фонда США CCF-2139462.

Литература

[1] Cohn R. M. Difference Algebra. — New York: Interscience, 1965.

[2] A. Einstein. The Meaning of Relativity. — Princeton, 1922. — P. 133—165 (Appendix II (Generalization of gravitation theory)).

[3] Kolchin E. R. The notion of dimension in the theory of algebraic differential equations // Bull. Amer. Math. Soc. — 1964. — Vol. 70. — P. 570—573.

[4] Kolchin E. R. Differential Algebra and Algebraic Groups. — Academic Press, 1973.

[5] Kondrateva M. V., Levin A. B., Mikhalev A. V., Pankratev E. V. Computation of dimension polynomials // Int. J. Algebra Comput. — 1992. — Vol. 2, no. 2. — P. 117—137.

[6] Kondrateva M. V., Levin A. B., Mikhalev A. V., Pankratev E. V. Differential and Difference Dimension Polynomials. — Kluwer Academic, 1998.

[7] Kondrateva M. V., Mikhalev A. V., Pankratev E. V. Jacobi's bound for independent systems of algebraic partial differential equations // Applicable Algebra Engin. Commun. Comput. — 2009. — Vol. 20, no. 1. — P. 65—71.

[8] Kondrateva M. V., Mikhalev A. V., Pankratev E. V. Jacobi's bound for systems of algebraic differential equations // J. Math. Sci. — 2009. — Vol. 163, no. 5. — P. 543—553.

[9] Levin A. B. Characteristic polynomials of inversive difference modules and some properties of inversive difference dimension // Russ. Math. Surv. — 1980. — Vol. 35, no. 1. — P. 217—218.

[10] Levin A. B. Computation of the strength of systems of difference equations via generalized Groebner bases // Groebner Bases in Symbolic Analysis. — Walter de Gruyter, 2007. — P. 43—73.

[11] Levin A. B. Gröbner bases with respect to several orderings and multivariable dimension polynomials // J. Symbol. Comput. — 2007. — Vol. 42. — P. 561—578.

[12] Levin A. B. Difference Algebra. — Springer, 2008.

[13] Levin A. B. Dimension polynomials of intermediate differential fields and the strength of a system of differential equations with group action // J. Math. Sci. — 2009. — Vol. 163, no. 5. — P. 554—562.

[14] Levin A. B. Multivariate dimension polynomials of inversive difference field extensions // Algebraic and Algorithmic Aspects of Differential and Integral Operators. — Springer, 2014. — (Lect. Notes Comput. Sci., Vol. 8372). — P. 146—163.

[15] Levin A. B. Dimension polynomials of difference local algebras // Adv. Appl. Math. — 2016. — Vol. 72. — P. 166—174.

[16] Levin A. B. Multivariate difference-differential dimension polynomials // Math. Comput. Sci. — 2020. — Vol. 14. — P. 361—374.

[17] Levin A. B. A new type of difference dimension polynomials // Math. Comput. Sci. — 2022. — Vol. 16. — No. 4, article 20.

[18] Levin A. B., Mikhalev A. V. Differential dimension polynomial and the strength of a system of differential equations // Computable Invariants in the Theory of Algebraic Systems. — Novosibirsk, 1987. — P. 58—66.

[19] Levin A. B., Mikhalev A. V. Dimension polynomials of filtered G-modules and finitely generated G-field extensions // Collection of Papers on Algebra. — Moscow State Univ., 1989. — P. 74—94.

[20] Levin A. B., Mikhalev A. V. Dimension polynomials of differential modules // Abelian Groups Modules. — 1989. — No. 9. — P. 51—67.

[21] Levin A. B., Mikhalev A. V. Dimension polynomials of difference-differential modules and of difference-differential field extensions // Abelian Groups Modules. — 1991. — No. 10. — P. 56—82.

[22] Levin A. B., Mikhalev A. V. Type and Dimension of Finitely Generated Vector G-spaces // Vestn. Mosk. Univ. Ser. 1 Mat. Mekh. — 1991. — No. 4. — P. 72—74.

[23] Levin A. B., Mikhalev A. V. Dimension polynomials of filtered differential G-modules and extensions of differential G-fields // Contemp. Math. — 1992. — Vol. 131, pt. 2. — P. 469—489.

[24] Levin A. B., Mikhalev A. V. Type and dimension of finitely generated G-algebras // Contemp. Math. — 1995. — Vol. 184. — P. 275—280.

[25] Mikhalev A. V., Pankratev E. V. Differential modules // Modules. Pt. 3. — Novosibirsk State Univ., 1973. — P. 14—21.

[26] Mikhalev A. V., Pankratev E. V. Differential dimension polynomial of a system of differential equations // Algebra. Collection of Papers. — Moscow State Univ., 1980. — P. 57—67.

[27] Mikhalev A. V., Pankratev E. V. Differential and difference algebra // J. Soviet Math. — 1989. — Vol. 45, no. 1. — P. 912—955

[28] Mikhalev A. V., Pankratev E. V. Computer Algebra. Calculations in Differential and Difference Algebra. — Moscow State Univ., 1989.

[29] Zhou M., Winkler F. Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules // J. Symbol. Comput. — 2008. — Vol. 43, no. 10. — P. 726—745.