Об обобщённой проблеме Ритта как вычислительной задаче*

О. Д. ГОЛУБИЦКИЙ
Университет Западного Онтарио, Канада
e-mail: Oleg.Golubitsky@gmail.com

М. В. КОНДРАТЬЕВА
Московский государственный университет им. М. В. Ломоносова
e-mail: kondratieva@sumail.ru

А. И. ОВЧИННИКОВ
Иллинойсский университет в Чикаго, США
e-mail: aiovchin@math.uic.edu

УДК 512.628

Ключевые слова: дифференциальная алгебра, проблема Ритта, разложение на простые компоненты.

Аннотация

Проблема Ритта заключается в возможности проверить, содержится ли один простой дифференциальный идеал в другом, если оба они заданы своими характеристическими множествами. Мы даём несколько эквивалентных формулировок этой проблемы. В частности, мы показываем, что проблема Ритта равносильна установлению факта, является ли дифференциальный многочлен делителем нуля по модулю радикального дифференциального идеала. Техника, использованная в доказательстве, позволяет получить алгоритмы для вычисления канонического разложения радикального дифференциального идеала на простые компоненты и нахождения канонической системы образующих. Предложенные представления радикального дифференциального идеала не зависят от выбора образующих и ранжира.

Abstract

O. D. Golubitsky, M. V. Kondratieva, A. I. Ovchinnikov, On the generalized Ritt problem as a computational problem, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 4, pp. 109—120.

The Ritt problem asks if there is an algorithm that decides whether one prime differential ideal is contained in another one if both are given by their characteristic sets. We give several equivalent formulations of this problem. In particular, we show that it is equivalent to testing whether a differential polynomial is a zero divisor modulo a radical differential ideal. The technique used in the proof of this equivalence yields algorithms for computing a canonical decomposition of a radical differential ideal into prime components and a canonical generating set of a radical differential ideal. Both proposed representations of a radical differential ideal are independent of the given set of generators and can be made independent of the ranking.

*Первый автор поддерживался грантом Совета по естественным наукам и исследованиям Канады PDF-301108-2004, третий автор — грантом Национального научного фонда США CCR-0096842.

Фундаментальная и прикладная математика, 2008, том 14, № 4, с. 109—120.

Посвящается памяти нашего научного руководителя, Е. В. Панкратьева

1. Введение

Проблема Ритта отражает следующее явление, характерное для алгебраических дифференциальных уравнений. Нетрудно убедиться, что множество решений дифференциального уравнения $y'^2 - 4y = 0$ состоит из семейства парабол и сингулярного нулевого решения. Множество решений уравнения $y'^2 - 4y^3 = 0$ составляют семейство гипербол и нулевое решение. Основное отличие между этими примерами заключается в том, что в первом случае сингулярное нулевое решение не является пределом главного семейства, в то время как во втором случае является. Говоря алгебраическим языком, дифференциальный идеал, порождённый первым уравнением, не является простым, в то время как идеал, порождённый вторым уравнением, прост. Исследование подобных свойств систем нелинейных алгебраических дифференциальных уравнений в частных производных и составляет проблему Ритта.

Рассмотрим кольцо дифференциальных многочленов над полем характеристики нуль. В классических работах Ритта показано, что каждый радикальный дифференциальный идеал может быть единственным образом представлен как пересечение конечного числа содержащих его минимальных простых дифференциальных идеалов, которые носят название существенных компонент. Задачу вычисления характеристических множеств существенных компонент данного радикального дифференциального идеала будем называть обобщённой проблемой Ритта. Она относится к нерешённым проблемам классической дифференциальной алгебры, и на сегодняшний день достигнут некоторый прогресс только в ряде частных случаев (см. [4, 5, 12, 14, 18]).

Мы дадим точную формулировку проблемы Ритта как вычислительной задачи сначала для некоторого класса дифференциальных полей, а затем сделаем её независимой от свойств поля. Одна из версий проблемы Ритта, которую мы здесь обсуждаем, формулируется в терминах делителей нуля по модулю радикального дифференциального идеала, другая — как проверка простоты идеала. Согласно определению, для проверки свойства простоты идеала необходимо уметь проверять для пары не принадлежащих идеалу многочленов, лежит ли их произведение в идеале. Мы сформулируем требуемое свойство в более простом виде, в терминах одного дифференциального многочлена.

Чтобы проиллюстрировать эти идеи, мы также представим алгоритм, который по заданной системе дифференциальных многочленов F строит набор характеристических множеств простых дифференциальных идеалов, обладающий следующими свойствами:

- радикальный дифференциальный идеал I, порождённый системой F, представляется в виде пересечения простых дифференциальных идеалов;
- это множество простых идеалов однозначно определено идеалом I и не зависит от выбора образующих F.

Мы надеемся, что предложенный в этой статье подход будет полезным для достижения прогресса в решении проблемы Ритта.

2. Основные определения

Пусть $\mathbf{k}$ — дифференциальное поле характеристики нуль с дифференцированиями $\Delta = \{\delta_1, \dots, \delta_m\}$. Пусть $Y = \{y_1, \dots, y_n\}$ — конечное множество дифференциальных неизвестных и

$$\Theta Y := \{\delta_1^{i_1} \cdot \ldots \cdot \delta_m^{i_m} y_j \mid i_k \geqslant 0,\ 1 \leqslant k \leqslant m,\ 1 \leqslant j \leqslant n\}.$$

Кольцо дифференциальных многочленов $\mathbf{k}\{Y\}$ представляет собой кольцо коммутативных многочленов от бесконечного множества обычных алгебраических неизвестных $\mathbf{k}[\Theta Y]$, дифференцирования из Δ продолжаются на него естественным образом.

Пусть I — радикальный дифференциальный идеал кольца $\mathbf{k}\{Y\}$, т. е. радикальный идеал, замкнутый относительно дифференцирований из Δ. Будем называть простой дифференциальный идеал P *существенной простой компонентой* идеала I, если $I \subseteq P$ и не существует простого дифференциального идеала Q, удовлетворяющего условию $I \subseteq Q \subsetneq P$. Согласно [18], каждый радикальный дифференциальный идеал I обладает конечным числом существенных простых компонент и их пересечение совпадает с ним; каждый простой дифференциальный идеал, содержащий I, содержит некоторую существенную компоненту I; любое множество простых дифференциальных идеалов, пересечение которых есть I, содержит в качестве подмножества набор существенных компонент. Представление радикального идеала в виде пересечения существенных компонент будем называть его несократимым представлением. *Обобщённая проблема Ритта* заключается в следующем: дан радикальный дифференциальный идеал, требуется найти все его существенные компоненты.

Для конструктивной формулировки этой проблемы фиксируем кодирование входных (радикальный дифференциальный идеал в $\mathbf{k}\{Y\}$) и выходных данных (конечное множество простых дифференциальных идеалов в $\mathbf{k}\{Y\}$). Радикальный дифференциальный идеал I обычно задаётся конечным множеством дифференциальных многочленов F, составляющих его базис. Мы будем записывать этот факт так: $I = \{F\}$. Через $[F]$ будет обозначать минимальный дифференциальный идеал, содержащий F. Для того чтобы можно было делать какие-то вычисления в кольце, мы будем предполагать, что $\mathbf{k}$ обладает некоторыми дополнительными свойствами. Следующее определение вводится в [17, определение 5] (см. [16]).

Определение 1. Дифференциальное кольцо R называется вычислимым, если существует вложение

$$i\colon R \to \mathbb{N},$$

такое что

1) образ $i(R)$ является рекурсивным подмножеством $\mathbb{N}$;

2) сложение, умножение и дифференцирование, индуцированные на этом образе соответствующими операциями кольца, являются вычислимыми функциями.

Вложение i из предыдущего определения называется *допустимой индексацией* R. Если $\mathbf{k}$ является вычислимым дифференциальным полем, то кольцо дифференциальных многочленов $\mathbf{k}\{Y\}$ также будет вычислимым дифференциальным кольцом: допустимую индексацию $j\colon \mathbf{k}\{Y\} \to \mathbb{N}$ для $f \in \mathbf{k}\{Y\}$ можно определить, исходя из значений индексаций $i\colon \mathbf{k} \to \mathbb{N}$ его коэффициентов (см. [17]).

Имея фиксированную индексацию j, мы можем сказать, что дифференциальный полином $f \in \mathbf{k}\{Y\}$ *задан*, если нам известно значение его индексации $j(f)$.

Простой дифференциальный идеал может задаваться двумя способами: либо порождающими элементами, либо характеристическим множеством. Последнее понятие определяется следующим образом. Рассмотрим ранжир на множестве ΘY, т. е. линейный порядок $\leqslant$ на нём, удовлетворяющий условиям

$$u \leqslant \delta u,\ u \leqslant v \implies \delta u \leqslant \delta v$$

для всех $u, v \in \Theta Y$, $\delta \in \Delta$. Для дифференциального полинома $f \in \mathbf{k}\{Y\} \setminus \mathbf{k}$ введём понятие лидера как самого старшего дифференциального неизвестного, входящего в f и обозначим его как $u = \mathrm{ld}_{\leqslant} f$. Если степень полинома f относительно u равна d, величину u^d назовём рангом f и будем обозначать через $\mathrm{rk}_{\leqslant} f$.

Дифференциальный полином f назовём редуцированным относительно дифференциального полинома g, если для любого дифференциального оператора $\theta \in \Theta$ степень f относительно лидера полинома θg меньше, чем степень θg относительно лидера θg. Множество дифференциальных полиномов назовём авторедуцированным, если любой его элемент редуцирован относительно любого другого. Отметим, что любое авторедуцированное множество является конечным.

Ранжир может быть расширен до сравнения рангов:

$$u_1^{d_1} \leqslant u_2^{d_2} \iff u_1 < u_2 \text{ либо } (u_1 = u_2 \text{ и } d_1 \leqslant d_2)$$

и до сравнения авторедуцированных множеств рангов: $R_1 \leqslant R_2$ равносильно либо условию $R_1 = R_2$, либо последнее неверно, но минимальный элемент симметричной разности $(R_1 \setminus R_2) \cup (R_2 \setminus R_1)$ принадлежит множеству R_1. Все три введённых выше порядка $\leqslant$ вполне упорядочивают соответствующие множества (дифференциальных переменных, рангов и авторедуцированных множеств рангов).

Ранжир нужен для конструктивного представления простого дифференциального идеала с помощью характеристического множества. Такое представление позволяет найти алгоритмы для решения многих проблем, например эффективно проверять принадлежность данного дифференциального полинома идеалу.

Среди авторедуцированных подмножеств данного множества дифференциальных многочленов X можно выбрать множество минимального ранга (так как множество авторедуцированных множеств рангов является вполне упорядоченным). Это множество называется характеристическим множеством X. Отметим, что характеристическое множество определяется неоднозначно, в то время как его ранг определён однозначно.

Рассмотрим дифференциальный многочлен f как многочлен от своего лидера u. Старший коэффициент f называется инициалом, а инициал любой собственной производной θf, где $\theta \in \Theta \backslash \{1\}$, называется сепарантой f. Для конечного множества $\mathcal{C}$ дифференциальных полиномов обозначим через $H_{\mathcal{C}}$ произведение инициалов и сепарант его элементов. Каждый простой дифференциальный идеал P полностью определяется своим характеристическим множеством (см., например, [12]), а именно имеет место представление идеала в виде дробного

$$P = [\mathcal{C}] : H_{\mathcal{C}}^{\infty}.$$

Мы будем постоянно использовать такое представление.

С другой стороны, если полином A неразложим, то идеал $[A] : H_A^{\infty}$ является простым и A — характеристическое множество этого простого идеала. Ритт поставил следующую задачу: определить, выполняется ли включение $[A] : H_A^{\infty} \subset \subset [y_1, \ldots, y_n]$, т. е. является ли точка $(0, \ldots, 0)$ общим нулём главной компоненты идеала $\{A\}$.

3. Основной результат

3.1. Различные формулировки проблемы Ритта

Мы дадим несколько эквивалентных формулировок проблемы Ритта и используем одну из них в попытке продвинуться в решении проблемы. Отметим, что эквивалентность имеет место для полей $\mathbf{k}$, удовлетворяющих условию *однозначности разложения на множители* полиномов от одной переменной $f \in \mathbf{k}[x]$, т. е. полей, для которых существует алгоритм, определяющий, является ли указанный многочлен f неприводимым. Это условие обычно используется для решения задач факторизации многочленов над полем $\mathbf{k}$ (см., например, [15,20]).

Примерами вычислимых полей, для которых выполняется условие однозначности разложения на множители, являются поля рациональных чисел и рациональных функций и их алгебраические замыкания. Пример вычислимого поля без данного условия дан в [15]: возьмём нерекурсивное, но рекурсивно перечислимое подмножество S натуральных чисел и рассмотрим $\mathbb{Q}[\sqrt{p_n} \colon n \in S]$, где p_n является n-м простым. Рассмотрев поле частных, мы получим пример нетривиального дифференциального поля, для которого не выполняется условие однозначности разложения на множители. Как и в [16, раздел 5], мы предлагаем рассматривать проблему Ритта, особенно её третью и четвёртую формулировку в следующей ниже теореме, как обобщение проблемы факторизации многочленов.

Теорема 1. *Следующие проблемы эквивалентны над вычислимым дифференциальным полем характеристики нуль, в котором выполняется условие однозначности разложения на множители* (*т. е. существование алгоритма для одной из них влечёт разрешимость всех остальных*).

1. *Дано характеристическое множество простого дифференциального идеала, требуется найти множество его образующих.*
2. *Даны характеристические множества двух простых дифференциальных идеалов I_1 и I_2, требуется определить, имеет ли место включение $I_1 \subset I_2$.*
3. *Вычислить несократимое простое разложение радикального дифференциального идеала.*
4. *Дано множество образующих радикального дифференциального идеала, требуется определить, является ли он простым.*
5. *Дано множество образующих радикального дифференциального идеала, требуется найти образующие каждой его простой компоненты* (*как радикального идеала*).
6. *Дано множество образующих радикального дифференциального идеала I и дифференциальный полином f, требуется определить, является ли f делителем нуля по модулю идеала I.*

Доказательство. $1 \Longrightarrow 2$. Предположим, что у нас есть алгоритм для нахождения образующих простого дифференциального идеала по его характеристическому множеству. Применим этот алгоритм к характеристическому множеству I_1, вычислим его образующие F_1, т. е. $I_1 = \{F_1\}$. Имеем $I_1 \subset I_2$ тогда и только тогда, когда $F_1 \subset I_2$.

$2 \Longrightarrow 3$. Пусть дан радикальный дифференциальный идеал $\{F\}$, мы можем применить к нему алгоритм Ритта—Колчина (см. [12, раздел IV.9], [13, алгоритм 5.5.15] или [19]), для того чтобы вычислить его разложение на простые компоненты $\{F\} = P_1 \cap \ldots \cap P_k$, где каждая простая компонента представляется своим характеристическим множеством.

Заметим, что для работы алгоритма Ритта—Колчина необходимо уметь проверять, является ли алгебраический идеал, представленный в форме $(\mathcal{C}) : H_{\mathcal{C}}^{\infty}$, где $\mathcal{C}$ — некоторое когерентное (см. [12, раздел III.8]) автоределуцированное множество, простым, и если нет, находить два полинома, не принадлежащих идеалу, произведение которых лежит в идеале. С таким тестом алгоритм Ритта—Колчина может применяться к любому вычислимому полю характеристики нуль.

Случай множества $\mathcal{C}$, состоящего из одного полинома от одной дифференциальной переменной, показывает, что условие существования алгоритма разложения на неприводимые множители над $\mathbf{k}$ является необходимым для упомянутого теста на простоту. Мы покажем, что это условие также является достаточным. Доказательство достаточности немного более сильного условия см. в [13, раздел 5.5] и [19].

В самом деле, если $\mathcal{C}$ является когерентным автоup редуцированным, то идеал $(\mathcal{C}) : H_{\mathcal{C}}^{\infty}$ будет радикальным [2,9]. Базис этого идеала может быть вычислен над любым вычислимым полем с помощью базиса Гребнера [1, раздел 4.4]. Образующие простых компонент идеала могут быть найдены над любым вычислимым полем, для которого выполняется условие разложения на неприводимые множители [6]. Если идеал имеет только одну простую компоненту, то он является простым. С другой стороны, выбрав в каждой простой компоненте многочлен, который не принадлежит никакой другой компоненте (что может быть сделано с помощью техники базисов Грёбнера в любом вычислимом поле), мы можем найти требуемое произведение.

Предположим, что у нас есть алгоритм для проверки того, что один простой дифференциальный идеал является подмножеством другого. Тогда в разложении на простые компоненты мы можем удалить лишние компоненты, т. е. такие P_i, которые содержат некоторые другие P_j. Оставшиеся компоненты будут существенными, поскольку любое простое разложение радикального идеала содержит все существенные компоненты. Таким образом, мы получим несократимое разложение радикального дифференциального идеала $\{F\}$.

$3 \Longrightarrow 4$. Предположим, что у нас имеется алгоритм разложения радикального дифференциального идеала $\{F\}$ на существенные компоненты. Тогда $\{F\}$ является простым в том и только том случае, когда разложение на существенные компоненты состоит ровно из одного идеала.

$4 \Longrightarrow 1$. Пусть дано характеристическое множество $\mathcal{C}$ простого дифференциального идеала P. Рассмотрим алгебраические идеалы $J_i = \left(\mathcal{C}^{(i)}\right) : H_{\mathcal{C}}^{\infty}$, $i = 0, 1, 2, \ldots$, где

$$\mathcal{C}^{(i)} = \{\theta f \mid \operatorname{ord} \theta \leqslant i,\ f \in \mathcal{C}\}.$$

Пусть F_i будет базисом Грёбнера идеала J_i. Согласно теореме о базисе существует такой индекс i, что $\{F_i\} = P$.

Предположим, что у нас есть алгоритм, способный проверять, является ли радикальный дифференциальный идеал $\{F\}$ простым. Применив этот алгоритм к $\{F_i\}$, $i = 0, 1, 2, \ldots$, найдём хотя бы один индекс i, такой что $\{F_i\}$ является простым. Так как $\mathcal{C}$ является характеристическим множеством $\{F_i\}$, будем иметь $\{F_i\} = P$, следовательно, F_i порождает P как простой дифференциальный идеал.

$1 \Longrightarrow 5$. Пусть дан радикальный дифференциальный идеал, применим алгоритм Ритта—Колчина для вычисления его простых компонент, представленных своими характеристическими множествами. Предположим, что у нас имеется алгоритм для вычисления образующих простого дифференциального идеала, заданного своим характеристическим множеством, и вычислим образующие каждой компоненты.

$5 \Longrightarrow 3$. Предположим, что у нас есть алгоритм для вычисления образующих простых компонент радикального дифференциального идеала. Тогда мы можем проверить наличие лишних компонент в простом разложении как в $1 \Longrightarrow 2$ и получить несократимое разложение как в $2 \Longrightarrow 3$.

$3 \Longrightarrow 6$. Предположим, что мы имеем алгоритм для вычисления существенных компонент $I = P_1 \cap \ldots \cap P_k$ радикального дифференциального идеала $I = \{F\}$.

Лемма 1. *Дифференциальный многочлен f является делителем нуля по модулю I тогда и только тогда, когда он принадлежит существенной простой компоненте I.*

Доказательство. Пусть f будет делителем нуля по модулю идеала I. Это означает, что существует дифференциальный многочлен $g \notin I$, такой что $fg \in I$. Так как $g \notin I$, то найдётся существенная простая компонента P_i идеала I, которая не содержит g. Условие $fg \in I$ влечёт $fg \in P_i$. Так как идеал P_i является простым, получим $f \in P_i$.

Пусть многочлен f принадлежит существенной простой компоненте идеала I. Обозначим через $P_{i_1}, \ldots, P_{i_l}$ существенные простые компоненты идеала I, которые не содержат f. Тогда для идеала $I : f = \{g \mid gf \in I\}$ будет выполняться

$$I : f = (P_1 \cap \ldots \cap P_k) : f = (P_1 : f) \cap \ldots \cap (P_k : f) = P_{i_1} \cap \ldots \cap P_{i_l}.$$

Так как $P_1 \cap \ldots \cap P_k$ — несократимое простое разложение идеала I, мы получим, что $I : f \neq I$, следовательно, f является делителем нуля по модулю идеала I. $\square$

Пример. Рассмотрим примеры, о которых шла речь во введении. Пусть $J_1 = \{y'^2 - 4y\}$, $J_2 = \{y'^2 - 4y^3\} \subset \mathbf{k}\{Y\}$. Простыми разложениями этих идеалов будут

$$J_1 = [y'^2 - 4y] : y'^\infty \cap [y], \quad J_2 = [y'^2 - 4y^3] : y'^\infty \cap [y].$$

Продифференцировав $y'^2 - 4y$, мы получим, что полином y' является делителем нуля по модулю J_1, и поэтому компонента $[y]$ является существенной для J_1. С другой стороны, согласно результатам Ритта (см. [18], немного другое доказательство этого же факта можно найти у Кона), для вычисления образующих главной компоненты уравнения первого порядка достаточно его продифференцировать столько раз, какова его степень. Вычислив базис Грёбнера алгебраического дробного идеала, получим, что для J_2 компонента y' не является существенной. По лемме 1 это означает, что y' по модулю J_2 не является делителем нуля, а J_2 прост.

$6 \Longrightarrow 1$. Эта импликация доказывается аналогично $4 \Longrightarrow 1$.

Пусть дано характеристическое множество $\mathcal{C}$ простого дифференциального идеала P. Рассмотрим алгебраические идеалы $J_i = \left(\mathcal{C}^{(i)}\right) : H_\mathcal{C}^\infty$, $i = 0, 1, 2, \ldots$. Пусть F_i будет системой образующих J_i. По теореме о базисе существует индекс i, такой что $\{F_i\} = P$. Заметим, что произведение $H_\mathcal{C}$ инициалов и сепарант $\mathcal{C}$ не является делителем нуля по модулю $\{F_i\}$, так как

$$P = \{F_i\} \subseteq \{F_i\} : H_\mathcal{C}^\infty \subseteq [\mathcal{C}] : H_\mathcal{C}^\infty = P.$$

Предположим, что у нас есть алгоритм, который может определять, является ли полином f делителем нуля по модулю радикального дифференциального идеала $\{F\}$. Применив этот алгоритм к $H_\mathcal{C}$ и $\{F_i\}$, $i = 0, 1, 2, \ldots$, найдём наименьший индекс i, такой что $H_{\mathcal{C}}$ не являлся делителем нуля по модулю $\{F_i\}$ (как было показано выше, такой индекс существует). Тогда $\{F_i\} : H_{\mathcal{C}}^{\infty} = \{F_i\}$. С другой стороны, $\{F_i\} : H_{\mathcal{C}}^{\infty} = P$, так как $\mathcal{C} \subset \{F_i\}$. Таким образом, $\{F_i\} = P$. □

3.2. Каноническое простое разложение радикального дифференциального идеала

В этом разделе мы покажем, как можно строить простое разложение радикального дифференциального идеала I, заданного множеством образующих F, которое не зависит от выбора конкретных образующих. Хорошим кандидатом на эту роль было бы разложение на существенные компоненты, но, как уже отмечалось, до сих пор неизвестно, является ли эта задача разрешимой. Наша конструкция базируется на двух простых замечаниях, содержащихся в лемме 2 и предложении 1.

Предположим, что ранжир фиксирован. Каждый простой дифференциальный идеал имеет однозначно определённое каноническое характеристическое множество (см. [3, 8, 10, 11]). Пусть дано множество $F \subset \mathbf{k}\{Y\}$, мы можем найти некоторое простое разложение

$$I = \{F\} = \bigcap_{i=1}^{k} [\mathcal{C}_i] : H_{\mathcal{C}_i}^{\infty}, \tag{1}$$

где $\mathcal{C}_i$ являются каноническими характеристическими множествами соответствующих простых дифференциальных идеалов.

Лемма 2. *Пусть $\mathcal{C}$ — характеристическое множество максимального ранга среди $\mathcal{C}_1, \ldots, \mathcal{C}_k$. Тогда идеал $P := [\mathcal{C}] : H_{\mathcal{C}}^{\infty}$ является существенной простой компонентой идеала I, имеющей наибольший ранг среди всех существенных простых компонент идеала I.*

Доказательство. Пусть $Q = [\mathcal{B}] : H_{\mathcal{B}}^{\infty}$, где $\mathcal{B}$ — каноническое характеристическое множество Q, является существенной простой компонентой идеала I, такой что $P \supseteq Q$. Ввиду этого включения и по определению характеристического множества как автоup редуцированного множества наименьшего ранга имеем $\operatorname{rk}\mathcal{C} \leqslant \operatorname{rk}\mathcal{B}$. Более того, так как Q является существенной простой компонентой идеала I, она должна встречаться среди идеалов $[\mathcal{C}_i] : H_{\mathcal{C}_i}^{\infty}$, $i = 1, \ldots, k$, а это значит, что $\mathcal{B} = \mathcal{C}_l$ для некоторого l, $1 \leqslant l \leqslant k$. Таким образом, согласно выбору $\mathcal{C}$ имеем $\operatorname{rk}\mathcal{C} \geqslant \operatorname{rk}\mathcal{B}$. Отсюда следует, что $\operatorname{rk}\mathcal{C} = \operatorname{rk}\mathcal{B}$. Таким образом, согласно [8, лемма 13] простые дифференциальные идеалы P и Q равны. □

Утверждение 1. *Пусть $I = \{F\}$ — радикальный дифференциальный идеал, и пусть $\mathcal{C} = C_1, \ldots, C_l$ — конечное множество дифференциальных многочленов, удовлетворяющих условию $\mathcal{C} \subset I \subset [\mathcal{C}] : H_{\mathcal{C}}^{\infty}$. Тогда**

$$I = [\mathcal{C}] : H_{\mathcal{C}}^{\infty} \cap I : C_1 \cap \ldots \cap I : C_l \cap \{F \cup H_{\mathcal{C}}\}.$$

*Допуская некоторую неточность, мы обозначаем через $F \cup H_{\mathcal{C}}$ объединение множества F и одноэлементного множества $H_{\mathcal{C}}$.

Доказательство. Пусть

$$f \in [\mathcal{C}] : H_{\mathcal{C}}^{\infty} \cap I : C_1 \cap \ldots \cap I : C_l \cap \{F \cup H_{\mathcal{C}}\}.$$

Тогда

$$C_i \cdot f \in I, \quad 1 \leqslant i \leqslant l,$$

и, следовательно, существует элемент $h \in H_{\mathcal{C}}^{\infty}$, такой что

$$h \cdot f \in [\mathcal{C}].$$

Мы имеем

$$h \cdot f^2 \in f \cdot [\mathcal{C}] \subset \{f \cdot C_1, \ldots, f \cdot C_l\} \subset I,$$

и следовательно, $f \in \{F\} : H_{\mathcal{C}}^{\infty}$. Так как выполняется

$$\{F\} = \{F\} : H_{\mathcal{C}}^{\infty} \cap \{F \cup H_{\mathcal{C}}\}$$

(см., например, [9, предложение 2.1]), мы видим, что $f \in I$. Обратное включение следует из $I \subset [\mathcal{C}] : H_{\mathcal{C}}^{\infty}$. □

Если в разложении (1) присутствуют несколько характеристических множеств максимального ранга, например $\mathcal{C}_1, \ldots, \mathcal{C}_q$, и $\mathcal{C}_i = C_{i,1}, \ldots, C_{i,p_i}$, $1 \leqslant i \leqslant q$, то

$$I = [\mathcal{C}_1] : H_{\mathcal{C}_1}^{\infty} \cap I : C_{1,1} \cap \ldots \cap I : C_{1,p_1} \cap \left\{F \cup H_{\mathcal{C}_1}\right\} \cap \ldots \cap \\ \cap [\mathcal{C}_q] : H_{\mathcal{C}_q}^{\infty} \cap I : C_{q,1} \cap \ldots \cap I : C_{q,p_q} \cap \left\{F \cup H_{\mathcal{C}_q}\right\}. \quad (2)$$

Заметим, что $\mathcal{C}_1, \ldots, \mathcal{C}_q$ и, следовательно, все идеалы в (2) однозначно определены идеалом I, иными словами, они не зависят от выбора образующих I. Более того, идеалы

$$I : C_{i,j} \quad (3)$$

и

$$\{F \cup H_{\mathcal{C}_i}\} \quad (4)$$

строго содержат I, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant p_i$. В самом деле, все $C_{i,j}$ являются элементами существенных простых компонент I, следовательно, $I : C_{i,j} \supsetneq I$. Так как $H_{\mathcal{C}_i}$ не принадлежит соответствующей существенной простой компоненте $[\mathcal{C}_i] : H_{\mathcal{C}_i}^{\infty}$, оно не принадлежит I и мы имеем $\{F \cup H_{\mathcal{C}_i}\} \supsetneq I$.

По теореме Ритта—Роденбаша любая строго возрастающая цепочка радикальный дифференциальных идеалов конечна. Следовательно, рекурсивно вычисляя каноническое, не зависящее от образующих простое разложение (3) и (4), мы получим не зависящее от выбора образующих разложение исходного идеала I. Заметим, что разложение на простые компоненты, которое требуется на шаге (1), может быть найдено для радикальных идеалов, заданных в дробном виде, как в (3).

3.3. Канонические разложения, не зависящие от ранжира и выбора образующих

Хотя каноническое разложение на простые компоненты методом, описанным в предыдущем разделе, не зависит от выбора образующих радикального идеала I, оно может зависеть от ранжира. Однако возможно получить разложение, которое не будет зависеть ни от ранжира, ни от образующих. Как и в (1), вычислим какое-нибудь простое разложение идеала I. Затем, вместо выбора характеристического множества максимального ранга относительно фиксированного ранжира (эта операция действительно от ранжира зависит), возьмём те простые компоненты, для которых существует *некоторый* ранжир, относительно которого каноническое характеристическое множество имеет максимальный ранг, и рассмотрим все *такие* характеристические множества $\mathcal{C}_1, \ldots, \mathcal{C}_q$. Этот шаг может быть выполнен путём вычисления универсального характеристического множества [7] для каждой простой компоненты. Остальные шаги выполняются без изменений.

Наконец, из канонического простого разложения

$$I = \bigcap_{i=1}^{k} [\mathcal{C}_i] : H_{\mathcal{C}_i}^{\infty}$$

можно получить каноническое множество образующих радикального дифференциального идеала, зависящее только от самого идеала. Для $j = 0, 1, 2, \ldots$ рассмотрим алгебраический идеал

$$I_j = \bigcap_{i=1}^{k} \bigl(\mathcal{C}_i^{(j)}\bigr) : H_{\mathcal{C}_i}^{\infty}$$

и вычислим его базис Грёбнера $\mathcal{B}_j$ относительно лексикографического упорядочения, индуцированного на произведениях элементов из ΘY ранжиром (если нам нужны не зависящие от ранжира образующие, рассмотрим универсальный базис Грёбнера). Остановимся на первом индексе j, таком что $\{\mathcal{B}_j\} = I$, и искомый $\mathcal{B}_j$ найден. Такой индекс j существует, поскольку $I = \bigcup\limits_{j=0}^{\infty} I_j$. Заметим, что совпадение двух радикальных идеалов, заданных своими образующими, может быть проверено путём тестирования каждой из образующих на принадлежность идеалу.

Мы признательны Майклу Сингеру и Вильяму Ситу за плодотворные дискуссии и поддержку, Расселу Миллеру за его объяснение теории вычислимых полей и последующие обсуждения связи этой теории с проблемой Ритта.

Литература

[1] Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. — М.: Мир, 2000.

[2] Boulier F., Lazard D., Ollivier F., Petitot M. Representation for the radical of a finitely generated differential ideal // ISSAC'95. Proc. 1995 Int. Symp. Symbolic and Algebraic Computation. — New York: ACM Press, 1995. — P. 158—166.

[3] Boulier F., Lemaire F. Computing canonical representatives of regular differential ideals // ISSAC'00. Proc. 2000 Int. Symp. Symbolic and Algebraic Computation. — New York: ACM Press, 2000. — P. 38—47.

[4] Cohn R. M. Specializations of differential kernels and the Ritt problem // J. Algebra. — 1979. — Vol. 61, no. 1. — P. 256—268.

[5] Cohn R. M. Valuations and the Ritt problem // J. Algebra. — 1986. — Vol. 101, no. 1. — P. 1—15.

[6] Eisenbud D., Huneke C., Vasconcelos V. Direct methods for primary decomposition // Invent. Math. — 1992. — Vol. 110. — P. 207—235.

[7] Golubitsky O. Gröbner fan and universal characteristic sets of prime differential ideals // J. Symbolic Comput. — 2006. — Vol. 41, no. 10. — P. 1091—1104.

[8] Golubitsky O., Kondratieva M. V., Ovchinnikov A. Algebraic transformation of differential characteristic decompositions from one ranking to another // J. Symbolic Comput. — 2009. — Vol. 44.

[9] Hubert E. Factorization-free decomposition algorithms in differential algebra // J. Symbolic Comput. — 2000. — Vol. 29, no. 4—5. — P. 641—662.

[10] Hubert E. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems // Symbolic and Numerical Scientific Computation. Second Int. Conf., SNSC 2001, Hagenberg, Austria, September 12—14, 2001 / F. Winkler, ed. — Berlin: Springer, 2003. — (Lect. Notes Comput. Sci.; Vol. 2630). — P. 1—39.

[11] Hubert E. Notes on triangular sets and triangulation-decomposition algorithms. II. Differential systems // Symbolic and Numerical Scientific Computation. Second Int. Conf., SNSC 2001, Hagenberg, Austria, September 12—14, 2001 / F. Winkler, ed. — Berlin: Springer, 2003. — (Lect. Notes Comput. Sci.; Vol. 2630). — P. 40—87.

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

[13] Kondratieva M. V., Levin A. B., Mikhalev A. V., Pankratiev E. V. Differential and Difference Dimension Polynomials. — Kluwer Academic, 1999.

[14] Levi H. On the structure of differential polynomials and on their theory of ideals // Trans. Amer. Math. Soc. — 1942. — Vol. 51. — P. 532—568.

[15] Miller R. G. Computable fields and Galois theory // Notices Amer. Math. Soc. — 2008. — Vol. 55, no. 7. — P. 798—807.

[16] Miller R. G. Computability and differential fields: A tutorial // Proc. Second Int. Workshop on Differential Algebra and Related Topics / L. Guo, W. Sit, eds. — 2008.

[17] Rabin M. O. Computable algebras, general theory and theory of computable fields // Trans. Amer. Math. Soc. — 1960. — Vol. 95, no. 2. — P. 341—360.

[18] Ritt J. F. Differential Algebra. — New York: Amer. Math. Soc., 1950.

[19] Sit W. Y. The Ritt—Kolchin theory for differential polynomials // Proc. Int. Workshop on Differential Algebra and Related Topics, Rutgers—The State University of New Jersey, New Brunswick, USA, November 2—3, 2000 / L. Guo, ed. — Singapore: World Scientific, 2002. — P. 1—70.

[20] Winkler F. Polynomial Algorithms in Computer Algebra. — Springer, 1996.