О периферийной факторизации линейных обыкновенных операторов *

С.А.Абрамов
ВЦ РАН, Москва
abramov@ccas.ru
С.П.Царев
КГПУ, Красноярск
tsarev@edk.krasnoyarsk.su

Аннотация

Разложение линейного обыкновенного дифференциального оператора на множители меньших порядков является важным инструментом анализа и решения дифференциальных уравнений. В статье обсуждаются классические и некоторые недавние результаты, касающиеся неоднозначности полной факторизации (т.е. разложения на неприводимые множители) линейных обыкновенных дифференциальных операторов, а также рассмотрен характер неоднозначности так называемой периферийной факторизации. Все обсуждаемые результаты верны не только для кольца дифференциальных операторов, но и, например, для колец разностных и q-разностных операторов. Более того, все рассуждения могут быть проведены для случая произвольного кольца полиномов Оре.

*Работа выполнена при частичной финансовой поддержке РФФИ и ИНТАС, грант 95-IN-RU-412.

1 Кольца операторов; факторизация

Пусть $\mathbf{K}$ — дифференциальное поле характеристики 0 с дифференцированием D. Таким образом, $D : \mathbf{K} \to \mathbf{K}$, причем $D(a+b) = Da + Db$, $D(ab) = (Da)b + a(Db)$ для любых $a, b \in \mathbf{K}$. Простой пример дает поле $\mathbf{K} = \mathbf{C}(x)$ (т.е. поле рациональных функций одной переменной с комплексными коэффициентами) с дифференцированием $D = \frac{d}{dx}$. Линейному обыкновенному дифференциальному уравнению

$$Ly = a_n D^n y + ... + a_1 Dy + a_0 y = 0, \tag{1}$$

для которого $a_1, ..., a_n \in \mathbf{K}$, соответствует линейный обыкновенный дифференциальный оператор

$$L = a_n D^n + ... + a_1 D + a_0, \tag{2}$$

являющийся элементом кольца $\mathbf{K}[D]$. Сложение в этом кольце определяется так же, как в кольце обычных полиномов. В то же время умножение $\circ$ в $\mathbf{K}[D]$ (некоммутативное) определяется, исходя из соотношения $D \circ (aD^m) = aD^{m+1} + (Da)D^m$, справедливого для всех $a \in \mathbf{K}$ и неотрицательных целых m.

Для теории алгебраических уравнений ключевую роль играет существование и единственность разложения на неприводимые множители в кольце обычных полиномов над произвольным полем. Напомним, что необратимый (т.е. такой, для которого не существует обратного) элемент кольца называется *неприводимым*, если в любом его разложении в произведение двух множителей из данного кольца один из этих множителей оказывается обратимым; в противном случае элемент называется *приводимым*.

В вопросах, связанных с поиском точных решений линейных дифференциальных уравнений в различных классах функций, разложение соответствующего оператора на множители также играет важную роль. В частности, сведéние поиска решения уравнения (1) к поиску решений уравнений меньших порядков путем разложения (2) широко используется в компьютерной алгебре. Последнее мы, с иллюстративными целями, рассмотрим более подробно.

Вопрос о том, как построить общее решение уравнения (1), решается особенно легко, если это общее решение задается в форме Даламбера

([1]), т.е. в виде

$$f_1 \int f_2 ... \int f_n \int 0 \tag{3}$$

при свободном выборе аддитивных постоянных интегралов (n - порядок уравнения). Здесь f_1 — частное решение уравнения (1); если понизить порядок (1) с помощью f_1 (т.е. применить подстановку Даламбера $y = f_1 \int u$, где u — новая неизвестная функция), то f_2 будет частным решением получившегося уравнения и т.д. В ([2]) показано, что если (3) - общее решение однородного уравнения (1), то общим решением неоднородного уравнения $Ly = g$ будет

$$f_1 \int f_2 ... \int f_n \int \frac{g}{a_n f_1 ... f_n},$$

где a_n - старший коэффициент L. Пусть $L = L_1 \circ L_2$ и $L, L_1, L_2 \in \mathbf{K}[D]$. Пусть $\operatorname{ord} L = n, \operatorname{ord} L_1 = s, \operatorname{ord} L_2 = t, n = s+t$. Пусть уравнение $L_1 y = 0$ имеет общее решение $\varphi_1 \int \varphi_2 ... \int \varphi_s \int 0$, и $L_2 = 0$ имеет общее решение $\psi_1 \int \psi_2 ... \int \psi_t \int 0$. Тогда, используя продемонстрированный выше прием построения общих решений неоднородных уравнений, можно получить общее решение уравнения (1) в виде

$$\psi_1 \int \psi_2 ... \int \psi_t \int \frac{\varphi_1}{b_t \psi_1 \cdots \psi_t} \int \varphi_2 ... \int \varphi_s \int 0,$$

где b_t - старший коэффициент оператора L_2. Эта формула допускает простое обобщение на произведение $L = L_1 \circ ... \circ L_k$ с произвольным k. Ее можно также применять последовательно, приняв в расчет, что $L = (L_1 \circ (L_2 \circ (\cdots \circ (L_{k-1} \circ L_k)...)))$.

Однако, для элементов $\mathbf{K}[D]$ не гарантируется единственность разложения на неприводимые множители. Пусть, например, $\mathbf{K} = \mathbf{C}(x), D = \frac{d}{dx}$, тогда

$$D^2 = (D + \frac{1}{x+c}) \circ (D - \frac{1}{x-c})$$

для любого $c \in \mathbf{C}$; можно допустить равенство $c = \infty$, считая, что оба множителя в правой части в этом случае равны D. Имеем

$$D^2 = D \circ D = (D + \frac{1}{x}) \circ (D - \frac{1}{x}) = (D + \frac{1}{x+1}) \circ (D - \frac{1}{x-1})$$

и т.д. Рассматривая какое-то одно разложение фиксированного оператора на неприводимые множители, приходится учитывать возможность такого рода неоднозначности. Для решения некоторых задач важна степень неоднозначности разложения, и желательно иметь представление о том, чем могут отличаться другие возможные разложения от данного. Может потребоваться ответ и на следующий вопрос: если имеющееся разложение недостаточно удобно для решения некоторой задачи, то можно ли рассчитывать на существование более удобного разложения?

Помимо разложения на неприводимые множители представляют интерес и разложения на множители некоторых специальных видов, причем некоторые из таких множителей могут быть приводимыми.

В настоящее время в литературе, и, в частности, в литературе по компьютерной алгебре, вместо термина "разложение на множители" часто прибегают к термину *факторизация.* Разложение на неприводимые множители называют *полной* факторизацией. В этой статье мы будем для краткости говорить просто о факторизации, подразумевая при этом полную факторизацию. Когда речь пойдет о факторизации, которая не является полной, мы будем давать соответствующие уточнения.

Одним из самых старых результатов, касающихся факторизаций, является теорема Э.Ландау ([3]) о том, что если

$$P_1 \circ ... \circ P_k \tag{4}$$

и

$$\overline{P}_1 \circ ... \circ \overline{P}_{\overline{k}} \tag{5}$$

— две различные факторизации одного и того же оператора L, то $k = \overline{k}$ и между множителями, входящими в первую и вторую факторизации, можно установить взаимно однозначное соответствие

$$P_i \leftrightarrow \overline{P}_{j_i}, \tag{6}$$

такое, что $\operatorname{ord} P_i = \operatorname{ord} \overline{P}_{j_i},\ i = 1, ..., k$. Разумеется, в некоторой конкретной факторизации могут встретиться совпадающие множители. Мы, однако, различаем операторы, имеющие разные порядковые номера.

В следующем разделе мы укажем более общие классические, а также некоторые недавние результаты, касающиеся вопроса о том, насколько сильно могут отличаться одна от другой две факторизации фиксированного оператора.

В последнем разделе мы рассмотрим разновидность факторизации, не являющейся полной (мы называем ее периферийной факторизацией). Свойства периферийной факторизации оператора L интересны, например, в связи с задачей фактического построения некоторой факторизации (т.е. некоторого полного разложения на неприводимые множители) оператора L. Алгоритмы факторизации [5, 7, 6] основываются на процедуре, позволяющей выяснить, имеет ли оператор $L, \operatorname{ord} L = n$, правый делитель заданного порядка m, и если да — то и найти один из таких делителей. Очевидно, что если у L нет правых делителей порядка $< m$, то каждый делитель порядка m будет неприводимым. Трудоемкость этой процедуры имеет быстрый рост при увеличении n и m. Поэтому если речь идет о нахождении какой-нибудь одной факторизации оператора L, то естественно попытаться первоначально отщепить от L побольше множителей невысокого порядка. Для того, чтобы применять упомянутую выше процедуру для поиска левых множителей, можно использовать сопряженный к L оператор L^* ([2, 5]) и учесть, что $L = AB$ тогда и только тогда, когда $L^* = B^*A^*$. После отщепления левых и правых множителей невысокого порядка поиск множителей более высокого порядка будет проводиться для оператора $\widetilde{L}, \operatorname{ord} \widetilde{L} = \widetilde{n}$, и возможно, что $\widetilde{n}$ окажется существенно меньше, чем n.

В связи со сказанным об убыстрении процесса поиска какой-то одной факторизации возникает вопрос: существует ли специальная стратегия отщепления левых и правых множителей, позволяющая добиваться того, чтобы получающаяся факторизация имела с левого и правого края (иными словами, на периферии) как можно больше множителей невысокого порядка? Ответ на этот вопрос оказывается отрицательным: чередовать отщепление левых и правых множителей и выбирать конкретные множители невысокого порядка можно произвольным образом. Для того, чтобы придать этому утверждению точную форму, требуется понятие периферийной факторизации и доказательство ряда связанных с этим понятием утверждений. Основным результатом данной статьи является теорема 4.

Все содержащиеся в этой статье результаты справедливы также для разностного и q-разностного случаев. Более того, эти результаты справедливы для случая произвольного кольца полиномов Оре ([4]). Привлекательность рассмотрения колец полиномов Оре состоит, с одной стороны, в том, что оно позволяет "одним махом" доказывать утверждения, касающиеся операторов разных видов. С другой стороны, использование этой теории позволяет создавать универсальные алгоритмы и соответствующие программы, настраиваемые на конкретный вид операторов и уравнений. Здесь укажем, что наряду с алгоритмами построения факторизаций для дифференциальных ([5, 7, 6]) и разностных ([8]) операторов, известен универсальный ("настраиваемый") алгоритм, работающий в произвольном кольце полиномов Оре ([9]). Приведем основное определение этой теории. Пусть $\mathbf{K}$ — поле характеристики 0, X — переменная, σ — автоморфизм поля $\mathbf{K}$ и δ — отображение $\mathbf{K} \to \mathbf{K}$, удовлетворяющее условию

$$\delta(a+b) = \delta a + \delta b, \ \delta(ab) = \sigma(a)\delta b + (\delta a)b$$

для любых $a, b \in \mathbf{K}$. Кольцом *полиномов Оре* (называемым также кольцом *косых полиномов*), заданным с помощью σ и δ, называется кольцо $\mathbf{K}[X; \sigma, \delta]$ полиномов от X, т.е. выражений вида

$$a_n X^n + ... + a_1 X + a_0, \tag{7}$$

в котором сложение — обычное, а умножение $\circ$ задано соотношением

$$X \circ a = \sigma(a)X + \delta a,$$

справедливым для любого $a \in \mathbf{K}$. *Порядком* полинома Оре (7) называется число n. Если $\mathbf{K}$ — дифференциальное поле с дифференцированием D, то соответствующее кольцо дифференциальных операторов реализуется как кольцо полиномов Оре с $\delta = D, \sigma = \epsilon$, где ϵ — тождественный автоморфизм поля $\mathbf{K}$. Если $\mathbf{K}$ — разностное поле со сдвигом E (содержательно: $Ef(x) = f(x+1)$), то соответствующее кольцо разностных операторов реализуется как кольцо полиномов Оре с $\delta = 0, \sigma = E$. Что касается q-разностного случая, то он очень схож с разностным: $\delta = 0, \sigma = Q$ (содержательно: $Qf(x) = f(qx)$). Представляет очевидный интерес кольцо полиномов Оре с $\delta = 0, \sigma = \Delta = E - \epsilon$ и т.д. Подробности можно найти в [4, 9] и, в частности — подробности о том, как определить действие полиномов Оре на элементы поля $\mathbf{K}$ или его расширения.

"Настраиваемость" программы, реализующей некоторый ориентированный на случай произвольного кольца полиномов Оре алгоритм, состоит в том, что предполагается процедурная конкретизация отображений σ и δ.

Все утверждения, которые приводятся в следующих разделах, можно интерпретировать как утверждения об операторах, являющихся элементами произвольного фиксированного кольца полиномов Оре. Но можно также, уходя от довольно абстрактных понятий, рассматривать их как утверждения о линейных обыкновенных дифференциальных операторах.

2 Перемещение множителей

Здесь мы изложим основы теории, развитой, главным образом, в работах А. Лёви и О. Оре [10, 11, 12, 13, 4]. Не нанося ущерба общности изложения, мы можем предполагать, что все рассматриваемые операторы таковы, что их старший коэффициент (т.е. a_n в (1) или в (7)) равен 1. Для любых двух ненулевых операторов L и M существует оператор, являющийся их *правым наибольшим общим делителем* $rGCD(L,M)$, т.е. оператор G такой, что для некоторых операторов L_1 и M_1 выполнено $L = L_1 \circ G$, $M = M_1 \circ G$ и порядок G максимален. Аналогичным образом, для L и M существует *правое наименьшее общее кратное* $rLCM(L,M)$, т.е. оператор K такой, что для некоторых операторов L_1 и M_1 выполнено $L_1 \circ L = M_1 \circ M = K$ и порядок K минимален. Имеет место равенство

$$\operatorname{ord} rLCM(L,M) = \operatorname{ord} L + \operatorname{ord} M - \operatorname{ord} rGCD(L,M).$$

По принятому нами соглашению считаем что старшие коэффициенты операторов $rGCD(L,M)$ и $rLCM(L,M)$ равны 1. Эти операторы для данных L и M определяются однозначно.

Говорят, что оператор L *сходен* с оператором M, если существует оператор R такой, что $rGCD(L,R) = 1$ и $rLCM(L,R) = M \circ R$. В этом случае любое решение $y(x)$ уравнения $Ly = 0$ отображается оператором R в решение $u = Ry$ уравнения $Mu = 0$. Доказывается, что сходные операторы имеют одинаковый порядок, и что оператор, сходный с неприводимым, сам неприводим. Сходство является отношением эквивалентности; для его обозначения мы будем использовать знак $\sim$ (будем писать $L \sim M$ и т.д.). Понятие сходства открывает возможность усилить теорему Ландау, упомянутую в разделе 1: доказывается, что взаимно однозначное соответствие (6) может быть выбрано таким, что $P_i \sim \overline{P}_{j_i}$.

Неприводимые операторы P и Q называются *взаимоперемещаемыми*, если существуют $\widetilde{P}$ и $\widetilde{Q}$ такие, что $P \neq \widetilde{Q}$ и $P \circ Q = \widetilde{Q} \circ \widetilde{P}$. Доказывается, что в этом случае $P \sim \widetilde{P}$, $Q \sim \widetilde{Q}$. Отметим, что понятие взаимоперемещамости несимметрично: если P и Q взаимоперемещаемы (в произведении $P \circ Q$), то Q и P (соответственно в произведении $Q \circ P$), вообще говоря, не взаимоперемещаемы. Понятие взаимоперемещаемости дает возможность доказать, что если даны две различные факторизации оператора L, то можно указать цепочку (конечную последовательность) факторизаций оператора L, концевые члены которой являются исходными факторизациями, и каждая последующая факторизация из цепочки отличается от предшествующей ей лишь в двух каких-то множителях. Последнее утверждение будет нами уточнено. Мы приведем его в виде теоремы, которая была доказана в [14] (более сильный вариант в сравнении с [10, 4]). Имеется в виду, что соответствие (6) можно выбрать так, что переход от (4) к (5) будет состоять в последовательных взаимных перемещениях смежных сомножителей, как при применении известного в теории сортировки метода пузырька. Последний метод в нашем случае выглядит следующим образом. Пометим операторы P_i их номерами i, а операторы $\overline{P}_1, \ldots, \overline{P}_k$ — соответствующими числами $j_1, \ldots, j_k$. Для большей наглядности перепишем (временно) рассматриваемые факторизации, проставляя пометы над операторами. Получим

$$\begin{pmatrix} 1 \\ P_1 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} k \\ P_k \end{pmatrix}, \tag{8}$$

и

$$\begin{pmatrix} j_1 \\ \overline{P}_1 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} j_k \\ \overline{P}_k \end{pmatrix}. \tag{9}$$

В первой факторизации возьмем оператор с пометой j_k, т.е. P_{j_k}. Перестановка $(j_1, \ldots, j_k)$, как утверждается, может быть выбрана так, что если $j_k \neq k$, то операторы P_{j_k} и P_{j_k+1} оказываются взаимоперемещаемыми: $P_{j_k} \circ P_{j_k+1} = \widetilde{P}_{j_k+1} \circ \widetilde{P}_{j_k}$. Можем перейти от (8) к

$$\begin{pmatrix} 1 \\ P_1 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} j_k - 1 \\ P_{j_k-1} \end{pmatrix} \circ \begin{pmatrix} j_k + 1 \\ \widetilde{P}_{j_k+1} \end{pmatrix} \circ \begin{pmatrix} j_k \\ \widetilde{P}_{j_k} \end{pmatrix} \circ \ldots \circ \begin{pmatrix} k \\ P_k \end{pmatrix}. \tag{10}$$

Теперь $\widetilde{P}_{j_k}$ и P_{j_k+2} оказываются взаимоперемещаемыми: $\widetilde{P}_{j_k} \circ P_{j_k+2} = \widetilde{P}_{j_k+2} \circ \widetilde{\widetilde{P}}_{j_k+2}$, и мы можем перейти от (10) к

$$\begin{pmatrix} 1 \\ P_1 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} j_k - 1 \\ P_{j_k-1} \end{pmatrix} \circ \begin{pmatrix} j_k + 1 \\ \widetilde{P}_{j_k+1} \end{pmatrix} \circ \begin{pmatrix} j_k + 2 \\ \widetilde{P}_{j_k+2} \end{pmatrix} \circ \begin{pmatrix} j_k \\ \widetilde{\widetilde{P}}_{j_k} \end{pmatrix} \circ \ldots \circ \begin{pmatrix} k \\ P_k \end{pmatrix}.$$

Оператор с пометой j_k будет перемещаться направо до тех пор, пока не достигнет правого края факторизации (здесь он становится равным $\overline{P}_k$). Мы получим факторизацию

$$\begin{pmatrix} 1 \\ P_1 \end{pmatrix} \circ ... \circ \begin{pmatrix} j_k - 1 \\ P_{j_k - 1} \end{pmatrix} \circ \begin{pmatrix} j_k + 1 \\ \widetilde{P}_{j_k+1} \end{pmatrix} \circ ... \circ \begin{pmatrix} k-1 \\ \widetilde{P}_{k-1} \end{pmatrix} \circ \begin{pmatrix} j_k \\ \overline{P}_k \end{pmatrix},$$

последний множитель которой совпадает с последним множителем факторизации (9).

После этого начинает перемещаться вправо оператор $P_{j_{k-1}}$ (точнее, оператор, помеченный числом j_{k-1}, так как в случае $j_{k-1} > j_k$ оператор $P_{j_{k-1}}$ преобразуется в $\widetilde{P}_{j_{k-1}}$ при предыдущих перемещениях оператора P_{j_k}), пока он не займет второе справа место (здесь он становится равным $\overline{P}_{k-1}$), и так далее. Такие перемещения операторов будем называть *пузырьковыми* перемещениями; предполагаем, что пометы перемещаются вместе с операторами.

Таким образом, существующая согласно обсуждаемой теореме перестановка $(j_1, ..., j_k)$ чисел $1, ..., k$, которая определяет взаимно однозначное соответствие (6), содержит в себе описание всего процесса перевода (8) в (9) пузырьковыми перемещениями.

Для этой теоремы мы приведем доказательство, ряд моментов которого позднее нами будет использован при доказательстве других утверждений. Экономя место, мы не будем надписывать в наших формулах пометы над операторами, а ограничимся краткими словесными пояснениями.

Теорема 1 ([14]) *Пусть (4) и (5) — две различные факторизации одного и того же оператора L. Тогда $k = \overline{k}$ и между множителями, входящими в первую и вторую факторизации, можно установить взаимно однозначное соответствие (6) такое, что факторизация (4) преобразуется в (5) пузырьковыми перемещениями.*

Доказательство проводится индукцией по порядку оператора L. Если $\operatorname{ord} L = 1$, то утверждение очевидно. Предполагая, что мы уже доказали наше утверждение для операторов L порядков $\leq n$, возьмем оператор $L = P_1 \circ \ldots \circ P_k = \overline{P}_1 \circ \ldots \circ \overline{P}_{\overline{k}}$ порядка $n+1$. Если P_k и $\overline{P}_{\overline{k}}$ совпадают, то мы можем сократить их, уменьшив порядок L. Если же P_k и $\overline{P}_{\overline{k}}$ не совпадают, то возьмем $R = rLCM(P_k, \overline{P}_{\overline{k}}) = S \circ P_k = T \circ \overline{P}_{\overline{k}}$. Операторы S и T неприводимы, так как $S \sim \overline{P}_{\overline{k}}$ и $T \sim P_k$. Очевидно, что R делит L:

$L = Q\circ R$ и мы имеем $L = P_1\circ\ldots\circ P_{k-1}\circ P_k = Q\circ R = Q_1\circ\ldots\circ Q_s\circ S\circ P_k = Q_1\circ\ldots\circ Q_s\circ T\circ \overline{P}_{\overline{k}} = \overline{P}_1\circ\ldots\circ\overline{P}_{\overline{k}-1}\circ\overline{P}_{\overline{k}}$, где Q_i дают разложение Q на неприводимые. Поскольку порядки $P_1\circ\ldots\circ P_{k-1} = Q_1\circ\ldots\circ Q_s\circ S$ и $Q_1\circ\ldots\circ Q_{k-2}\circ T = \overline{P}_1\circ\ldots\circ\overline{P}_{\overline{k}-1}$ не превосходят n, имеем $s+1 = k-1$, $s+1 = \overline{k}-1$, т.е. $\overline{k} = k, s = k-2$. Мы получаем, таким образом, $P_1\circ\ldots\circ P_{k-1} = Q_1\circ\ldots\circ Q_s\circ S$, и можно найти серию пузырьковых перемещений, преобразующих левую часть этого равенства в правую. Возьмем первый этап этой серии, когда оператор P_m, помеченный той же пометой, что и S, последовательно перемещается в произведении $P_1\circ\ldots\circ P_{k-1}$, направо (и преобразуется в S). После этого первого этапа получаем разложение $L = \widetilde{Q}_1\circ\ldots\circ\widetilde{Q}_{k-2}\circ S\circ P_k$. Далее выполним взаимное перемещение S и P_k в этом разложении, получив $L = \widetilde{Q}_1\circ\ldots\circ\widetilde{Q}_{k-2}\circ T\circ\overline{P}_k$. Тем самым мы определили для оператора $\overline{P}_k$ помету m. По индукции мы можем теперь выбрать пометы операторов $\overline{P}_i$, $i < k$, так, что существует последовательность пузырьковых перемещений, преобразующих $\widetilde{Q}_1\circ\ldots\circ\widetilde{Q}_{k-2}\circ T$ в $\overline{P}_1\circ\ldots\circ\overline{P}_{k-1}$. Мы определили все пометы исходных операторов $\overline{P}_i$ (пометами операторов $P_1,\ldots,P_k$ являются, соответственно, числа 1, ..., k) и нужную серию пузырьковых перемещений, последовательно преобразующих факторизации оператора L: $P_1\circ\ldots\circ P_{k-1}\circ P_k \longrightarrow \widetilde{Q}_1\circ\ldots\circ\widetilde{Q}_{k-2}\circ S\circ P_k \longrightarrow \widetilde{Q}_1\circ\ldots\circ\widetilde{Q}_{k-2}\circ T\circ\overline{P}_k \longrightarrow \overline{P}_1\circ\ldots\circ\overline{P}_{k-1}\circ\overline{P}_k$. $\Box$

Оператор L называется *вполне приводимым*, если он может быть представлен как правое наименьшее общее кратное некоторого количества неприводимых операторов, $L = rLCM(P_1,\ldots,P_k)$.

Как можно показать ([4]), в этом случае $L = \overline{P}_1\circ\ldots\overline{P}_{k-1}\circ P_k$, где $\overline{P}_s \sim P_s$, $s = 1,\ldots,k-1$.

Теорема 2 ([4]) *Необходимым и достаточным условием того, чтобы оператор был вполне приводим, является взаимоперемещаемость любых двух смежных неприводимых множителей в любой факторизации этого оператора.* $\Box$

Нам понадобится также

Теорема 3 *Пусть $L = rLCM(P,Q)$, и $P = P_1\circ\ldots\circ P_k$, $Q = Q_1\circ\ldots\circ Q_m$ — факторизации P и Q. Тогда множители любой факторизации $L = L_1\circ\ldots\circ L_n$ можно поставить во взаимно однозначное соответствие некоторому подмножеству объединения $\{P_1,\ldots,P_k\}\cup\{Q_1,\ldots,Q_m\}$, так,* *что оператор, соответствующий L_i, будет сходен с L_i (и, в частности, иметь тот же порядок).*

Доказательство. Разложим следующими двумя способами L на неприводимые множители: $L = A \circ Q = B \circ P = A_1 \circ \ldots \circ A_p \circ Q_1 \circ \ldots \circ Q_m = B_1 \circ \ldots \circ B_t \circ P_1 \circ \ldots \circ P_k$. Существует последовательность пузырьковых перемещений, переводящая $A_1 \circ \ldots \circ A_p \circ Q_1 \circ \ldots \circ Q_m$ в $B_1 \circ \ldots \circ B_t \circ P_1 \circ \ldots \circ P_k$. Выберем среди A_i все те, которые помечены теми же числами, что и операторы P_j. В последовательности пузырьковых перемещений произведем теперь те и только те, которые перемещают выбранные A_i вправо до тех пор, пока они не будут собраны вместе (в некотором порядке) у левой границы произведения $Q = Q_1 \circ \ldots \circ Q_m$ (но не перейдут ее): $L = \widetilde{A}_1 \circ \ldots \circ \widetilde{A}_q \circ \widetilde{A}_{q+1} \circ \ldots \circ \widetilde{A}_p \circ Q$, где $\widetilde{A}_{q+1}, \ldots, \widetilde{A}_p$ — выбранные. Это, очевидно, возможно, поскольку оставшиеся A_j имеют пометы, соответствующие операторам B_l, т.е. переставляются позднее; перемещения среди Q_i пока не производим, ибо они не влияют на взаимоперемещаемость A_j. Теперь, как очевидно, разложение оператора $L_1 = \widetilde{A}_{q+1} \circ \ldots \circ \widetilde{A}_p \circ Q_1 \circ \ldots \circ Q_m$ может быть преобразовано серией пузырьковых перемещений в $L_1 = X_1 \circ \ldots X_r \circ P_1 \circ \ldots \circ P_k$, $r = p + m - k$. Мы видим, что L_1 делится на P и Q, следовательно $q = 0$, так как L является правым наименьшим общим кратным P и Q. Отсюда, применяя теорему 1, получаем требуемое утверждение. $\square$

3 Периферийная факторизация

Определим

$$\mathcal{F}_{\mathbf{K}}^m = \{P | P \text{ — неприводимый оператор, } \operatorname{ord} P \leq m\}.$$

Пусть $L \in \mathbf{K}[D]$ и при этом L равен

$$L_1 \circ \ldots \circ L_l \circ U \circ R_r \circ \ldots \circ R_1, \tag{11}$$

где L_i, $R_j \in \mathcal{F}_{\mathbf{K}}^m$, а оператор U (вообще говоря, приводимый) не имеет левых и правых делителей, принадлежащих $\mathcal{F}_{\mathbf{K}}^m$. Тогда (11) определяет для L *периферийную* факторизацию порядка m.

Количество l левых или r правых множителей может, вообще говоря, отличаться в различных периферийных факторизациях (заданного порядка m) одного и того же оператора: взяв в качестве L наименьшее общее кратное нескольких неприводимых операторов из $\mathcal{F}^m_{\mathbf{K}}$ и одного неприводимого оператора порядка $m+1$, легко построить, пользуясь теоремой 2 и перемещая множители из $\mathcal{F}^m_{\mathbf{K}}$, различные периферийные факторизации порядка m этого оператора L с различными числами l, r (но одинаковой суммой $l+r$).

Теорема 4 *Пусть (11) и $\overline{L}_1 \circ \ldots \circ \overline{L}_{\overline{l}} \circ \overline{U} \circ \overline{R}_{\overline{r}} \circ \ldots \circ \overline{R}_1$ — две различные периферийные факторизации порядка m одного и того же оператора L. Тогда $r+l = \overline{r}+\overline{l}$, и общее количество множителей данного порядка среди L_i, R_i и среди $\overline{L}_j$, $\overline{R}_j$ совпадает.*

Доказательство теоремы вытекает из следующих лемм.

Лемма 1 *Пусть $L = V \circ R_s \circ \ldots \circ R_1$, где $R_1, \ldots, R_s \in \mathcal{F}^m_{\mathbf{K}}$, и V не имеет правых делителей из $\mathcal{F}^m_{\mathbf{K}}$. Пусть $V = L_1 \circ \ldots \circ L_t \circ U$, где $L_1, \ldots, L_t \in \mathcal{F}^m_{\mathbf{K}}$, и U не имеет левых делителей из $\mathcal{F}^m_{\mathbf{K}}$. Тогда s и t не зависят от выбора $L_1, \ldots, L_t, R_1, \ldots, R_s$ и оператор U определен однозначно.*

Доказательство. Если мы имеем $L = V \circ R_s \circ \ldots \circ R_1 = \overline{V} \circ \overline{R}_{\overline{s}} \circ \ldots \circ \overline{R}_1$, то оператор L делится справа на $M = rLCM(R_s \circ \ldots \circ R_1, \overline{R}_{\overline{s}} \circ \ldots \circ \overline{R}_1)$. В силу теоремы 3, $M = A_1 \circ \ldots \circ A_\alpha \circ R_s \circ \ldots \circ R_1 = B_1 \circ \ldots \circ B_\beta \circ \overline{R}_{\overline{s}} \circ \ldots \circ \overline{R}_1$, где $\alpha, \beta \geq 0$ и все A_i, $B_j \in \mathcal{F}^m_{\mathbf{K}}$. Поскольку V и $\overline{V}$ не имеют правых делителей из $\mathcal{F}^m_{\mathbf{K}}$, множители A_j, B_i должны отсутствовать, $M = R_s \circ \ldots \circ R_1 = \overline{R}_{\overline{s}} \circ \ldots \circ \overline{R}_1$, и в силу теоремы 1, $s = \overline{s}$, $V = \overline{V}$. Аналогичное рассуждение применяем к U. □

Утверждение последней леммы верно также после перехода от правых делителей к левым, а от левых - к правым.

Лемма 2 *Пусть $L = L_1 \circ \ldots \circ L_m \circ T$ и $L = S \circ R$, где $L_1, \ldots, L_m, R \in \mathcal{F}^m_{\mathbf{K}}$. Тогда $S = L'_1 \circ \ldots \circ L'_{m-1} \circ V$, где $L'_1, \ldots, L'_{m-1} \in \mathcal{F}^m_{\mathbf{K}}$.*

Доказательство. Разложив на множители T и S, имеем $L = L_1 \circ \ldots \circ L_m \circ T_1 \circ \ldots \circ T_t = S_1 \circ \ldots \circ S_s \circ R$. Найдем последовательность пузырьковых перемещений, переводящую первое разложение во второе. Если оператору R соответствует (т.е. имеет ту же помету) какой-то оператор T_r, то совершая соответствующие пузырьковые перемещения, в которых участвует этот оператор, получим $L = L_1 \circ \ldots \circ L_m \circ T_1 \circ \ldots \circ T_t = L_1 \circ \ldots \circ L_m \circ T_1 \circ \ldots \circ T_{r-1} \circ \overline{T}_{r+1} \circ \ldots \circ \overline{T}_t \circ R$, откуда $S = L_1 \circ \ldots \circ L_m \circ T_1 \circ \ldots \circ T_{r-1} \circ \overline{T}_{r+1} \circ \ldots \circ \overline{T}_t$, и утверждение леммы в этом случае доказано ($V = L_m \circ T_1 \circ \ldots \circ T_{r-1} \circ \overline{T}_{r+1} \circ \ldots \circ \overline{T}_t$). Если R соответствует некоторому L_r, аналогичная серия пузырьковых перемещений $L = L_1 \circ \ldots \circ L_{r-1} \circ \overline{L}_{r+1} \circ \ldots \circ \overline{L}_m \circ \overline{T}_1 \circ \ldots \circ \overline{T}_t \circ R$, откуда получаем требуемое разложение: $S = L_1 \circ \ldots \circ L_{r-1} \circ \overline{L}_{r+1} \circ \ldots \circ \overline{L}_m \circ \overline{T}_1 \circ \ldots \circ \overline{T}_t$, $V = L_1 \circ \ldots \circ L_{r-1} \circ \overline{L}_{r+1} \circ \ldots \circ \overline{L}_m$. □

Утверждение последней леммы верно также после перехода от левых делителей L_i к правым, и от правого делителя R к левому.

Лемма 3 *Пусть $L_1, \ldots, L_s, R_1, \ldots, R_t \in \mathcal{F}^m_{\mathbf{K}}$ и пусть операторы U, V не имеют ни левых, ни правых делителей в $\mathcal{F}^m_{\mathbf{K}}$. Пусть*

$$L_1 \circ \ldots \circ L_s \circ U = V \circ R_t \circ \ldots \circ R_1. \tag{12}$$

Тогда $s = t$.

Доказательство. Предположим противное; пусть, например, $t < s$. Тогда, используя лемму 2 (и замечание, сделанное после ее доказательства), мы можем преобразовать левую часть (12) к виду $L'_1 \circ \ldots \circ L'_{s-t} W R_t \circ \ldots \circ R_1$. Тогда $L'_1 \circ \ldots \circ L'_{s-t} W = V$, но V не имеет левых делителей из $\mathcal{F}^m_{\mathbf{K}}$.□

Пусть m фиксировано. Будем говорить, что периферийная факторизация (11) имеет *тип* (l, r).

Лемма 4 *Пусть оператор L допускает периферийную факторизацию типа $(u, 0)$. Тогда для любой периферийной факторизации оператора L некоторого типа (a, b) верно, что $a + b = u$.*

Доказательство. Пусть $L = L'_1 \circ \ldots \circ L'_u \circ S = L_1 \circ \ldots \circ L_a \circ T \circ R_b \circ \ldots \circ R_1$. Используя лемму 1 (и замечание, сделанное после ее доказательства), получаем, что $u \geq a$ и $L'_1 \circ \ldots \circ L'_u = L_1 \circ \ldots \circ L_a \circ L_{a+1} \circ \ldots \circ L_u$ для некоторых $L_{a+1}, \ldots, L_u \in \mathcal{F}^m_{\mathbf{K}}$. Это дает

$$L_{a+1} \circ \ldots \circ L_u \circ S = T \circ R_b \circ \ldots \circ R_1.$$

По лемме 3 получим $u - a = b$, т.е. $u = a + b$. □

Теперь мы можем доказать теорему 4. Рассмотрим разложение вида (11) и построим еще одно разложение: $L = L'_1 \circ \ldots \circ L'_t \circ V \circ R_s \circ \ldots \circ R_{r+1} \circ R_r \circ \ldots \circ R_1$, $s \geq r$, где $L'_1 \circ \ldots \circ L'_t \circ V$ не имеет правых делителей из $\mathcal{F}^m_{\mathbf{K}}$. Тогда $L'_1 \circ \ldots \circ L'_t \circ V \circ R_s \circ \ldots \circ R_{r+1} = L_1 \circ \ldots \circ L_l \circ U$ и в силу леммы 4, $t + (s - r) = l$, т.е. $t + s = l + r$. Но в силу леммы 1 s и t определены однозначно. □

Замечание. Как очевидно из доказательства, верно несколько более сильное утверждение, получающееся заменой определения $\mathcal{F}^m_{\mathbf{K}}$ на другое. Именно, мы можем выбрать в качестве $\mathcal{F}^m_{\mathbf{K}}$ любое множество неприводимых операторов, включающее наряду с любым своим элементом также все операторы, сходные с ним. Например, можно взять $\mathcal{F}^m_{\mathbf{K}}$, состоящее из всех операторов, сходных с некоторым данным неприводимым L_0.

Литература

[1] С.А. Абрамов, Подстановки Даламбера и сопряженные дифференциальные уравнения (компьютерно-алгебраический аспект), *Ж. вычисл. матем. и матем. физ.*, 1994, т.34, N^o 7, С. 1001–1014.

[2] S.A. Abramov & M. Petkovšek, D'Alembertian solutions of linear differential and difference equations. *Proc. ISSAC'94*, 1994, p. 169–174.

[3] E. Landau, Über irreduzible Differentialgleichungen. *J. für die reine und angewandte Mathematik*, 1902, v. 124, p. 115–120.

[4] O. Ore, Theory of non-commutative polynomials. *Annals of Mathematics*, 1933, v. 34, p. 480–508.

[5] F. Schwarz, Efficient factorization of liner ODE's. *SIGSAM Bulletin*, 1994, v. 28, N^o 1, p 9–17.

[6] С.П.Царев, О некоторых задачах, возникающих при факторизации линейных обыкновенных дифференциальных операторов, *Программирование*, 1994, N^o 1, с. 45–48.

[7] M. Bronstein, An improved algorithm for factoring linear ordinary differential operatorsin. *Proc. ISSAC'94*, 1994, p. 336–340.

[8] M. Petkovšek, Factorization of Linear Difference Operators. *University Of Ljubljana. Preprint series*, Vol. 30, 364, 1992.

[9] M. Bronstein & M. Petkovšek , An introduction to pseudo–linear algebra. *Theoretical Computer Science*, v.157, 1996, p. 3–33

[10] A. Loewy, Über reduzible lineare homogene Differentialgleichungen. *Math. Annalen*, 1903, v. 56, p. 549–584.

[11] A. Loewy, Über vollstandig reduzible lineare homogene Differentialgleichungen. *Math. Annalen*, 1906, v. 62, p.89–117.

[12] O. Ore, Formale Theorie der linearen Differentialgleichungen (Erster Teil). *J. für die reine und angewandte Mathematik*, 1932, v. 167, p. 221–234.

[13] O. Ore, Formale Theorie der linearen Differentialgleichungen (Zweiter Teil). *J. für die reine und angewandte Mathematik*, 1932, v. 168, p. 233–252.

[14] S.P. Tsarev, An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator, *Proc. ISSAC'96*, 1996, p. 226–231.