КОЛЬЦА МНОГОЧЛЕНОВ ОРЕ ОДНОЙ ПЕРЕМЕННОЙ В КОМПЬЮТЕРНОЙ АЛГЕБРЕ

С. А. АБРАМОВ, Х. К. ЛЕ (H. Q. LE), AND З. ЛИ (Z. LI)

Аннотация. Мы описываем несколько алгоритмов, относящихся к кольцам многочленов Оре (или, для краткости, кольцам Оре), и Maple-пакет, реализующий основные операции в произвольном кольце Оре. Этот пакет можно использовать в качестве базового для многих алгоритмов в кольцах Оре, в частности, в дифференциальных кольцах, кольцах со сдвигом и кольцах с q-сдвигом.

1. Введение

Теория колец Оре (или, то же самое, колец многочленов Оре) дает возможность рассматривать обыкновенные линейные дифференциальные, разностные, q-разностные и другие операторы с общей точки зрения. Эти кольца были предложены Оре [24, 25, 26] как основа единой теории факторизации операторов, обобщающей теорию, разработанную ранее Ландау и Лёви для дифференциального случая [17, 21, 22]. Способ интерпретации абстрактных многочленов Оре как линейных операторов на векторном пространстве был предложен Джекобсоном в [16].

Теория колец Оре хороша не только тем, что позволяет одним махом доказывать утверждения об операторах разного вида, но также и открываемой ею возможностью создания многоцелевых алгоритмов и соответствующих программ, которые можно настраивать на конкретный вид операторов и уравнений. Стоит упомянуть, что идея привлечения колец Оре в компьютерной алгебре впервые была высказана и использована Бронштейном и Петковшеком в статье [8], где описан алгоритм факторизации в произвольном кольце Оре.

В этой работе мы описываем некоторые (но далеко не все) алгоритмы компьютерной алгебры, относящиеся к кольцам Оре. Раздел 2 содержит обзор

колец многочленов Оре одной переменной. В разделе 3, посвященном сопряжённым операторам, материал изложен в более общем виде, чем ранее [3]; материал раздела 4 об эффективном вычислении наибольших общих делителей (gcd) и наименьших общих кратных (lcm) излагается впервые. В разделе 5 даётся обзор пакета `OreTools`, который позволяет работать с многочленами Оре от одной переменной в системе компьютерной алгебры Maple [23]. Этот пакет можно использовать в качестве базы для многих алгоритмов в кольцах Оре, в частности, в дифференциальных кольцах, кольцах со сдвигом E и кольцах с q-сдвигом Q.

Сравнение этого пакета с другими подобными пакетами проводится в разделах 4 и 6. Информация о доступе к пакету приведена в разделе 7.

2. Кольца многочленов Оре одной переменной

В разделах 2.1, 2.4 дается краткий обзор общей теории многочленов Оре одной переменной и соответствующих линейных операторов. Детальное обсуждение и доказательства соответствующих утверждений см. в [24, 16, 8]. В разделе 2.2 мы рассматриваем идею гильбертова упрощения, следуя описанию из [10, 8]. В разделе 2.3 приводятся определение и основные свойства сопряжённых многочленов (детали см. в [10, Гл. 1 и 8 (разд. 3)]).

2.1. **Многочлены Оре.** Пусть k — поле характеристики 0, а $\sigma : k \to k$ — автоморфизм k.

Определение 2.1. Дифференцирование относительно σ — это любое отображение $\delta : k \to k$, для которого

$$\delta\,(a+b) = \delta\,a + \delta\,b \text{ и } \delta\,(ab) = \sigma(a)\,\delta\,b + \delta a\,b \text{ для любых } a, b \in k. \tag{1}$$

Определение 2.2. Множество констант (относительно σ и δ) — это

$$\mathrm{Const}_{\sigma,\delta}(k) = \{a \in k \,:\, \sigma(a) = a,\, \delta a = 0\}.$$

Можно показать, что $\mathrm{Const}_{\sigma,\delta}(k)$ — подполе поля k.

Следующая лемма описывает связь между σ и δ. Если не возникает путаницы, мы обозначаем 1 тождественное отображение на k.

Лемма 2.1. *Пусть δ — дифференцирование k относительно σ.*

(i) *Если* $\sigma \neq 1$, *то существует элемент* $\alpha \in k$, *для которого* $\delta = \alpha(\sigma - 1)$.

(ii) *Если* $\delta \neq 0$, *то существует элемент* $\beta \in k$, *для которого* $\sigma = \beta\,\delta + 1$.

Пример 2.1. Пусть $k = \mathbb{F}(t)$ в случаях 1–4 и $k = \mathbb{F}(q, t)$ в случаях 5–7, где $\mathbb{F}$ — любое подполе $\mathbb{C}$.

	Случай	σ	δ
1	дифференциальный	1	$\frac{d}{dt}$
2	эйлеров дифференциальный	1	$t\frac{d}{dt}$
3	рекуррентный	E	0
4	разностный	E	$E-1$
5	q-рекуррентный	Q	0
6	q-разностный	Q	$Q-1$
7	q-дифференциальный	Q	$\frac{Q-1}{t(q-1)}$

Определение 2.3. Кольцо Оре (многочленов одной переменной) над k, заданное посредством σ и δ и обозначаемое $k[x; \sigma, \delta]$, — это кольцо многочленов от x над k с обычным сложением многочленов и умножением, заданным формулой

$$x\,a = \sigma(a)\,x + \delta a \quad \text{для любого } a \in k. \tag{2}$$

Элементы кольца $k[x; \sigma, \delta]$ называются многочленами Оре. Заметим, что в качестве k можно рассматривать некоторое кольцо (мы будем рассматривать многочлены Оре над кольцами в разделах 2.4, 3 и 4).

Пусть $p(x) \in k[x; \sigma, \delta]$ и $p(x) = p_m x^m + \cdots + p_1 x + p_0$, $p_m \neq 0$, тогда $m = \deg p(x)$, $p_m = \operatorname{lc} p(x)$. Положим $\deg 0 = -\infty$, $\operatorname{lc} 0 = 0$. Если $\operatorname{lc} p(x) = 1$, то многочлен $p(x)$ называется *унитарным*. Можно показать, что в $k[x; \sigma, \delta]$ имеются алгоритмы правого и левого деления. Пусть $a, b \in k[x; \sigma, \delta] \setminus \{0\}$. Применяя алгоритм правого деления, мы получаем

$$a = q_1\,b + r_1, \;\; q_1, r_1 \in k[x; \sigma, \delta], \;\; \deg\, r_1 < \deg\, b;$$

r_1, q_1 называются соответственно *правым остатком* и *правым частным* при делении a на b. Аналогично, применяя алгоритм левого деления, мы получаем

$$a = b\,q_2 + r_2, \;\; q_2, r_2 \in k[x; \sigma, \delta], \;\; \deg\, r_2 < \deg\, b;$$

r_2, q_2 называются соответственно *левым остатком* и *левым частным* при делении a на b.

Для данных $a, b \in k[x;\sigma,\delta]$ можно найти *наибольший общий правый делитель* (gcrd) правым алгоритмом Евклида и *наименьшее общее левое кратное* (lclm) *расширенным* правым алгоритмом Евклида. Вычисление *наибольшего общего левого делителя* (gcld) и, соотв., *наименьшего общего правого кратного* (lcrm) можно свести к вычислению gcrd и, соотв., lclm использованием сопряжения.

2.2. **Гильбертово упрощение.** Гильбертово упрощение — это изоморфизм колец, который отображает произвольное кольцо Оре в кольцо Оре с с тривиальным дифференцированием при условии, что σ нетривиален.

Предложение 2.2. *Если существует $\alpha \in k$, для которого $\alpha \neq \sigma(\alpha)$, то биекция $H_\alpha : k[x;\sigma,\delta] \to k[y;\sigma,0]$, заданная формулой*

$$H_\alpha\left(\sum_i a_i x^i\right) = \sum_i a_i \left(\frac{y+\delta\alpha}{\alpha-\sigma(\alpha)}\right)^i,$$

является изоморфизмом колец.

2.3. **Сопряжённые многочлены.**

Определение 2.4. Пусть $k[x;\sigma,\delta]$ — кольцо Оре. Сопряжённое к $k[x;\sigma,\delta]$ кольцо Оре — это $k[x;\sigma^*,\delta^*]$, где

$$\sigma^* = \sigma^{-1}, \;\; \delta^* = -\delta\,\sigma^{-1}. \tag{3}$$

Пусть $a = a_n\,x^n + \cdots + a_1\,x + a_0 \in k[x;\sigma,\delta]$. Сопряжённый многочлен a^* определяется как

$$a^* = x^n\,a_n + \cdots + x\,a_1 + a_0 \in k[x;\sigma^*,\delta^*].$$

Отметим, что произведение $x^i\,a_i$ надо вычислять в кольце Оре $k[x;\sigma^*,\delta^*]$. Легко показать, что $\mathrm{Const}_{\sigma,\delta}(k) = \mathrm{Const}_{\sigma^*,\delta^*}(k)$ и $(\sigma^*)^* = \sigma$, $(\delta^*)^* = \delta$. Также можно проверить, что сопряжение — линейное (над $\mathrm{Const}_{\sigma,\delta}$) биективное отображение и $(a^*)^* = a$, $(ab)^* = b^*a^*$. Кроме того,

$$\mathrm{gcld}(a,b) = (\mathrm{gcrd}(a^*,b^*))^*, \quad \mathrm{lcrm}(a,b) = (\mathrm{lclm}(a^*,b^*))^*.$$

Пример 2.2. Из примера 2.1 и определения 2.4 следует, что

	Случай	σ^*	δ^*
1	дифференциальный	1	$-\frac{d}{dt}$
2	эйлеров дифференциальный	1	$-t\,\frac{d}{dt}$
3	рекуррентный	E^{-1}	0
4	разностный	E^{-1}	$E^{-1}-1$
5	q-рекуррентный	Q^{-1}	0
6	q-разностный	Q^{-1}	$Q^{-1}-1$
7	q-дифференциальный	Q^{-1}	$\frac{Q^{-1}-1}{t(q-1)}$

2.4. **Многочлены Оре как линейные операторы.**

Определение 2.5. Пусть V — векторное пространство над k. Отображение $\theta : V \to V$ псевдолинейно относительно σ и δ, если

$$\theta(u+v) = \theta(u) + \theta(v), \quad \theta(a\,u) = \sigma(a)\,\theta(u) + \delta a\,u \tag{4}$$

для любых $a \in k$, $u, v \in V$.

Предположим, что K — σ,δ-согласованное надкольцо k, т. е. σ и δ продолжаются соответственно до автоморфизма кольца K и его дифференцирования относительно σ. Мы также предположим, что $\mathrm{Const}_{\sigma,\delta}(K) = \mathrm{Const}_{\sigma,\delta}(k)$, и будем использовать обозначение C для этого поля. Заметим, что K — векторное пространство над k, и, следовательно, может играть роль V. Мы будем рассматривать псевдолинейные отображения из K в K, предполагая, что соотношения (4) выполнены для любых $a, u, v \in K$.

Лемма 2.3. *Для любого $c \in K$ отображение $\theta_c : K \to K$, заданное формулой*

$$\theta_c(a) = c\,\sigma(a) + \delta a, \tag{5}$$

K-псевдолинейно относительно σ и δ, и $\theta_c(1) = c$. Наоборот, для любого K-псевдолинейного отображения θ элемент $c = \theta(1)$ таков, что отображение θ совпадает с θ_c, определённым в (5).

Рассмотрим кольцо $k[\theta]$ C-линейных операторов $L : K \to K$ вида $L = p(\theta)$, $p(x) \in k[x;\sigma,\delta]$. Соответствие $p(x) \to p(\theta)$ даёт нам гомоморфизм колец $\Theta : k[x;\sigma,\delta] \to k[\theta]$ благодаря псевдолинейности θ. Мы предположим, что

$$p(\theta) \text{ — нулевой оператор на } K \iff p(x) \text{ — нулевой многочлен Оре,} \tag{6}$$

и, как следствие, соответствие $p(x) \to p(\theta)$ задаёт изоморфизм колец. Если $L = p(\theta)$, то мы положим $\operatorname{ord} L = \deg p$.

Иногда удобно рассматривать также кольца $K[x; \sigma, \delta]$ и $K[\theta]$. Мы предположим, что для них выполнено (6).

Легко привести пример, который показывает, что (6) не выполнено в общем случае (скажем, $K = k = \mathbb{C}$, $\sigma(z) = \bar{z}$, $\delta = 0$, $\theta = \sigma$). В предложении 3.2 мы сформулируем простое и естественное достаточное условие выполнения (6).

Как следствие лемм 2.1 и 2.3 мы получаем

Предложение 2.4. *Отображение θ, K-псевдолинейное относительно σ и δ, равно $\delta + \theta(1)$, если $\sigma = 1$, и $(\theta(1) + \alpha)\sigma - \alpha$, если $\sigma \neq 1$, при этом α определено в лемме 2.1 (i).*

Условие (6) не выполнено в случае $\theta(1) + \alpha = 0$ (иначе $\theta + \alpha = 0$), так что мы заключаем, что если $\sigma \neq 1$, то $\theta(1) + \alpha \neq 0$. Мы дополнительно предположим, что $\theta(1) + \alpha$ не есть делитель нуля в K (это выполнено, напр., если $\theta(1) \in k$ и, как следствие, $\theta(1) + \alpha \in k$).

Пример 2.3. Псевдолинейные отображения θ и константы $c = \theta(1)$:

	Случай	θ	c
1	дифференциальный	$\frac{d}{dt}$	0
2	эйлеров дифференциальный	$t\,\frac{d}{dt}$	0
3	рекуррентный	E	1
4	разностный	$E - 1$	0
5	q-рекуррентный	Q	1
6	q-разностный	$Q - 1$	0
7	q-дифференциальный	$\frac{Q-1}{t(q-1)}$	0

3. Сопряжённые операторы

3.1. **Оператор ∇.** Пусть θ — псевдолинейное отображение из K в K относительно σ, δ. Положим $\nabla = \theta - \theta(1)$, $\nabla \in K[\theta]$. По предложению 2.4

$$\nabla = \begin{cases} \delta, & \text{если } \sigma = 1, \\ (\theta(1) + \alpha)(\sigma - 1), & \text{если } \sigma \neq 1, \end{cases}$$

а по лемме 2.1 и потому, что $\theta(1)+\alpha$ не есть делитель нуля, для любого $f \in K$

$$\nabla(f) = 0, \text{ если и только если } f \in C. \tag{7}$$

Легко вывести отсюда, что при $L \in K[\theta]$ выполнено $L(1) = 0$, если и только если существует $M \in K[\theta]$, для которого $L = M\nabla$. Учитывая вдобавок то, что $L(f) = (Lf)(1)$, и условие (6), мы получаем

Предложение 3.1. *Пусть $p \in K[x;\sigma,\delta]$, $L = p(\theta), f \in K$. Тогда $L(f) = 0$, если и только если существует $M \in K[\theta]$, для которого $Lf = M\nabla$, т. е. если и только если pf делится справа на $x - \theta(1)$.*

Пусть $c = \theta(1)$ и $p \in K[x;\sigma,\delta] \setminus \{0\}$, $\deg p = d$, тогда существует неотрицательное целое n, для которого $p = (b_{d-n}(x-c)^{d-n} + \cdots + b_1(x-c) + b_0)(x-c)^n$, где $b_0, \ldots, b_{d-n} \in K$, $b_0 \neq 0$. Это даёт нам

Предложение 3.2. *Предположим, что для любого неотрицательного целого n существует $f \in K$, для которого $\nabla^n(f) \in C \setminus \{0\}$. Тогда (6) выполнено для любого $p \in K[x;\sigma,\delta]$.*

Пример 3.1. Продолжение примера 2.3:

	Случай	∇
1	дифференциальный	$\frac{d}{dt}$
2	эйлеров дифференциальный	$t\,\frac{d}{dt}$
3	рекуррентный	$E-1$
4	разностный	$E-1$
5	q-рекуррентный	$Q-1$
6	q-разностный	$Q-1$
7	q-дифференциальный	$\frac{Q-1}{t(q-1)}$

3.2. **Сопряжённые операторы и интегрирующие множители.** По лемме 2.3 $\theta = \theta_c = c\,\sigma + \delta$, где $c = \theta(1)$. Положим $\theta^* = c\,\sigma^* + \delta^*$, где σ^*, δ^* — как в (3). Заметим, что $\theta(1) = c = \theta^*(1)$.

Определение 3.1. Пусть $k[x;\sigma,\delta]$ — кольцо Оре, θ — псевдолинейное отображение относительно σ, δ. Сопряжённое к $k[\theta]$ кольцо определяется как кольцо операторов $k[\theta^*]$. Если $p \in k[x;\sigma,\delta]$ и $L = p(\theta)$, то сопряжённый к L оператор определяется как $L^* = p^*(\theta^*) \in k[\theta^*]$.

Имеем $(LM)^* = M^*L^*$ для любых $L, M \in k[\theta]$. Если мы предположим, что (6) выполнено для $K[x;\sigma^*,\delta^*]$ и $K[\theta^*]$, то вдобавок $(L^*)^* = L$ для любого $L \in k[\theta]$.

Рассмотрим оператор $\nabla^* = \theta^* - \theta(1) = \theta^* - \theta^*(1)$. По предложению 3.1 $L^*(f) = 0$, если и только если существует $M \in K[\theta^*]$, для которого $L^*f = M\nabla^*$, т. е. $fL = \nabla M^*$. Это даёт нам

Предложение 3.3. *Пусть $p \in K[x;\sigma,\delta]$, $L = p(\theta), f \in K$. Тогда $L^*(f) = 0$, если и только если существует $N \in K[\theta]$, для которого $fL = \nabla N$, т. е. если и только если fp делится слева на $x - \theta(1)$.*

Предложения 3.1 и 3.3 представляют собой аналог теоремы Безу для алгебраических уравнений с одним неизвестным.

Пример 3.2. Продолжение примеров 2.2 и 2.3:

	Случай	θ^*	∇^*
1	дифференциальный	$-\frac{d}{dt}$	$-\frac{d}{dt}$
2	эйлеров дифференциальный	$-t\,\frac{d}{dt}$	$-t\,\frac{d}{dt}$
3	рекуррентный	E^{-1}	$E^{-1}-1$
4	разностный	$E^{-1}-1$	$E^{-1}-1$
5	q-рекуррентный	Q^{-1}	$Q^{-1}-1$
6	q-разностный	$Q^{-1}-1$	$Q^{-1}-1$
7	q-дифференциальный	$\frac{Q^{-1}-1}{t(q-1)}$	$\frac{Q^{-1}-1}{t(q-1)}$

Естественно назвать *интегрирующим множителем* для L любой $f \in K$, для которого $fL = \nabla N$, $N \in K[\theta]$. Предложение 3.3 — аналог классической теоремы из теории обыкновенных дифференциальных уравнений, но формулировка этого предложения дана в общей “форме Оре".

Пример 3.3. Пусть $k = \mathbb{C}(n), \sigma = \theta = E, \delta = 0$, $\nabla = E - 1$, K — кольцо последовательностей с элементами из $\mathbb{C}$. Рассмотрим оператор

$$L = (n+4)\,E^2 + E - (n+1) \in k[\theta].$$

Соответствующее сопряжённое уравнение $L^*(f) = 0$ — это

$$L^*(f) = -(n+1)\,f(n) + f(n-1) + (n+2)\,f(n-2) = 0. \tag{8}$$

Если интегрирующий множитель f для L является гипергеометрическим термом, то его можно найти, применяя алгоритм Hyper [28] к (8); это применение проходит успешно и даёт $f = (-1)^n$. Как следствие,

$$(-1)^n L = (E-1)((-1)^{n-1}(n+3)E + (-1)^n(n+1)).$$

3.3. **Аккуратное интегрирование.** Элемент $g \in K$ — *первообразный* для $f \in K$, если $\nabla(g) = f$. Предположим, что $\theta(1) \in k$ (т. е. $\nabla \in k[\theta]$) и рассмотрим следующую задачу: пусть заданы $f \in K$ и минимальный аннулирующий оператор $L \in k[\theta]$ для f (значение $n = \operatorname{ord} L$ — минимальное с тем свойством, что $L \in k[\theta]$ и $L(f) = 0$). Определить, существует ли такой первообразный элемент g элемента f, для которого минимальный аннулирующий оператор $\tilde{L}$ имеет порядок n. Если это так, то построить такой g и его минимальный аннулирующий оператор.

Эта задача (задача *Аккуратного интегрирования*) была решена в [3]. Сопряжённые операторы играют ключевую роль в решении. Мы приводим ниже краткое описание алгоритма. Заметим, что в [3] описание дано в двух (главных) случаях: $\sigma = 1, \theta = \delta$ и $\theta = \sigma - 1, \delta = 0$. Если задача имеет положительное решение (существует оператор $\tilde{L}$ порядка n), то алгоритм строит $r \in k[\theta]$, $\operatorname{ord} r = n - 1$, для которого $g = r(f)$, вместе с $\tilde{L}$.

В [3] было показано, что $\tilde{L}$, для которого $\operatorname{ord} \tilde{L} = n$, существует, если и только если уравнение $L^*(y) = 1$ имеет решение l в k. В этом случае r таково, что $1 - lL = \nabla r$ (так что r можно найти левым делением) и $\tilde{L} = 1 - r\nabla$. Если такого l не существует, то интегрирующий оператор r также не существует, в то время как минимальный аннулирующий оператор $\tilde{L}$ для g равен $L\nabla$, $\operatorname{ord} \tilde{L} = n + 1$.

Как замечено в [3], этот алгоритм обобщает алгоритм Госпера для неопределённого гипергеометрического суммирования [14] в двух смыслах: (а) он решает аналогичную задачу для более широкого класса уравнений, (б) он работает для любого порядка n, а не только для $n = 1$.

Пример 3.4. Мы покажем в этом примере использование аккуратного интегрирования в вычислении первообразных для выражений, включающих в себя присоединенные функции Лежандра первого и второго рода:

$$p_1 = (27\,t^2+4)^{5/4}\,\mathcal{P}^{5/2}_{2/3\sqrt{7}-1/2}\left(-\frac{3}{2}\sqrt{3}i\,t\right),$$

$$p_2 = (27\,t^2+4)^{5/4}\,\mathcal{Q}^{5/2}_{2/3\sqrt{7}-1/2}\left(-\frac{3}{2}\sqrt{3}i\,t\right).$$

Как p_1, так и p_2 аннулируются дифференциальным оператором

$$L = \left(27\,t^2+4\right)D^2 - 81\,tD + 24.$$

Соответствующее сопряжённое уравнение $L^*(y) = 1$ — это

$$\left(27\,t^2+4\right)\frac{d^2}{dt^2}y\,(t) + 189\,t\frac{d}{dt}y\,(t) + 159\,y(t) = 1,$$

оно имеет рациональное решение $l = 1/159$ (решения, имеющие вид рациональных функций, могут быть найдены алгоритмом из [1]). Значит, оператор $r \in k[\theta]$, для которого $\int p_1 dt = r(p_1)$ и $\int p_2 dt = r(p_2)$, — это левое частное от деления $1 - lL$ на ∇, которое равно

$$\left(-\frac{9}{53}\,t^2 - \frac{4}{159}\right)D + \frac{45}{53}t.$$

Заметим, что ни Maple 8, ни Mathematica 4 не могут вычислить два этих неопределённых интеграла.

4. Новые модулярные методы вычисления **gcd** и **lcm**

Обычное коммутативное кольцо многочленов $k[x]$ — это частный случай колец многочленов Оре. Многие эффективные методы для коммутативного случая были обобщены на некоммутативные $k[x;\sigma,\delta]$ (см. [15, 19, 20, 12]). В этом разделе мы предлагаем новые модулярные методы вычисления gcrd и lclm многочленов Оре. Для применения модулярных методов требуются небольшие ограничения на поле коэффициентов. Пусть $\mathbb{D}$ — либо кольцо целых чисел $\mathbb{Z}$, либо кольцо многочленов от нескольких переменных над $\mathbb{Z}$. Пусть t — новая переменная над $\mathbb{D}$, а $\mathbb{D}[t]$ — кольцо обычных коммутативных многочленов от t над $\mathbb{D}$. Мы будем работать в кольце Оре $\mathbb{D}[t][x;\sigma,\delta]$, у которого кольцо констант содержит $\mathbb{D}$. Заметим, что σ — автоморфизм $\mathbb{D}[t]$.

4.1. **Вычисление gcrd.** Пусть p простое. Гомоморфизм колец ϕ_p из $\mathbb{D}[t]$ в $\mathbb{Z}_p[t]$ называется *модулярным относительно* σ, если $\phi_p(\mathbb{D}) = \mathbb{Z}_p$, $\phi_p(t) = t$ и $\deg_t(\sigma(t)) = \deg_t \phi_p(\sigma(t))$. Определим автоморфизм σ_p на $\mathbb{Z}_p[t]$ как переводящий t в $\phi_p(\sigma(t))$, а любой элемент $\mathbb{Z}_p$ — в себя. Далее, определим аддитивное отображение δ_p из $\mathbb{Z}_p[t]$ в себя как переводящее t^n в $\phi_p(\delta(t^n))$ при $n \in \mathbb{N}$. Непосредственно проверяется, что диаграммы

$$\begin{array}{ccc} \mathbb{D}[t] & \xrightarrow{\sigma} & \mathbb{D}[t] \\ \downarrow \phi_p & & \downarrow \phi_p \\ \mathbb{Z}_p[t] & \xrightarrow{\sigma_p} & \mathbb{Z}_p[t] \end{array} \qquad \begin{array}{ccc} \mathbb{D}[t] & \xrightarrow{\delta} & \mathbb{D}[t] \\ \downarrow \phi_p & & \downarrow \phi_p \\ \mathbb{Z}_p[t] & \xrightarrow{\delta_p} & \mathbb{Z}_p[t] \end{array}$$

коммутативны и что $\mathbb{Z}_p[t][x, \sigma_p, \delta_p]$ — кольцо Оре. Модулярный гомоморфизм ϕ_p можно продолжить до отображения из $\mathbb{D}[t][x, \sigma, \delta]$ в $\mathbb{Z}_p[t][x, \sigma_p, \delta_p]$, переводящего $\sum_i a_i x^i$ в $\sum_i \phi_p(a_i) x^i$, где $a_i \in \mathbb{D}[t]$. Это продолженное отображение также будет обозначаться ϕ_p, и то, что оно является гомоморфизмом колец, устанавливается прямой проверкой.

Пусть e — элемент $\mathbb{Z}_p$. Под отображением вычисления ψ_e из $\mathbb{Z}_p[t]$ в $\mathbb{Z}_p$ мы понимаем отображение, которое переводит $\sum_i m_i t^i$ в $\sum_i m_i e^i$, где $m_i \in \mathbb{Z}_p$. Такое отображение вычисления можно продолжить до отображения из $\mathbb{Z}_p[t][x, \sigma_p, \delta_p]$ в $\mathbb{Z}_p[x]$, переводящего $\sum_i a_i x^i$ в $\sum_i \psi_e(a_i) x^i$, где $a_i \in \mathbb{Z}_p[t]$. Это продолженное отображение снова обозначается ψ_e.

Пример 4.1. Рассмотрим дифференциальное кольцо $D = \mathbb{Z}_p[t][x; 1, \frac{d}{dt}]$ и отображение вычисления ψ_e. Если ψ_e — гомоморфизм колец из D в $\mathbb{Z}_p[x]$ с как-либо определённым умножением, то тогда $\psi_e(xt) = \psi_e(tx + 1) = ex + 1$, и, с другой стороны,

$$\psi_e(xt) = \psi_e(x)\psi_e(t) = xe = x(\underbrace{1 + \cdots + 1}_{e \text{ раз}}) = ex.$$

Это приводит к противоречию.

Итак, как бы мы ни определили умножение в $\mathbb{Z}_p[x]$, ψ_e обычно не является гомоморфизмом колец. Это лишь гомоморфизм модулей (гомоморфизм левого модуля $\mathbb{Z}_p[t][x]$ над $\mathbb{Z}_p[t]$ в $\mathbb{Z}_p[t]$ над $\mathbb{Z}_p$).

Ключевая задача в модулярных gcrd-методах — это

Задача E. По данным P_1, P_2 в $\mathbb{Z}_p[t][x, \delta_p, \sigma_p]$ и отображению вычисления ψ_e вычислить образ $\operatorname{gcrd}(P_1, P_2)$ под действием ϕ_e.

Алгоритм GCRD_e, описанный в [20], решает задачу E. Пусть $\deg P_i = n_i$, $i = 1, 2$, $n = \max(n_1, n_2)$, $n_t = \max(\deg_t P_1, \deg_t P_2)$ и $G = \operatorname{gcrd}(P_1, P_2)$ имеет степень g. Число ψ_e, для которых GRCD_e выдаёт неправильные образы или ошибку, не превосходит $(n_1 + n_2)n_t$. Следовательно, GCRD_e выдаёт достаточно много правильных образов для процесса комбинирования, когда простое p достаточно велико. Сложность GCRD_e близка к $\left(n_t n^2 + n^3\right)$ в дифференциальном случае. Слагаемое n^3 происходит из редукции строк в матрице Сильвестра для P_1 и P_2, в которой $(n_1 + n_2)$ строк и $(n_1 + n_2)$ столбцов. Мы изложим улучшенный вариант алгоритма GCRD_e, сложность которого ограничена сверху величиной $\left(n_t(n-g)^2 + (n-g)^3\right)$. Это улучшение позволяет нашему модулярному методу для gcrd эффективно работать, когда g велико. В общих чертах, улучшенный алгоритм — это тщательно спланированный процесс редукции строк в матрице, ассоциированной с $\operatorname{sres}_{g-1}(P_1, P_2)$, в которой $n_1 + n_2 - 2(g-1)$ строк и $n_1 + n_2 - g + 2$ столбцов.

Чтобы описать улучшение, условимся о терминологии. Мы отсылаем читателя к [19] за определением субрезультантов P_1 и P_2 и связанными с этим обозначениями. Напомним, что m-й субрезультант P_1 и P_2 обозначается S_m для $m = n_2, n_2 - 1, \ldots, 0$. Пара последовательных субрезультантов S_m и S_{m+1} называется *gcrd-парой* P_1 и P_2 *с индексом* m, если $\deg S_m = m$ и $S_{m+1} = 0$. Непосредственно из теоремы 4.2 работы [19] и структуры пропусков в цепочке субрезультантов следует

Предложение 4.1. *Пусть P_1, P_2 в $\mathbb{Z}_p[t][x, \delta_p, \sigma_p]$ имеют степени n_1 и n_2 соответственно, где $n_1 \geq n_2 > 0$. Тогда P_1 и P_2 имеют gcrd-пару, если и только если* gcrd *P_1 и P_2 имеет положительную степень. Если gcrd-пара существует, то она единственна.*

При заданной последовательности

$$x^{n_2-1}P_1, \ldots, xP_1, P_1, \; x^{n_1-1}P_2, \ldots, xP_2, P_2, \tag{9}$$

отображение вычисления ψ_e называется *собственным* относительно P_1 и P_2, если

$$\deg \psi_e(x^i P_1) = (n_1 + i) \quad \text{при } i = 0, \ldots, (n_2 - 1) \text{ и}$$

$$\deg \psi_e(x^j P_2) = (n_2 + j) \quad \text{при } j = 0, \ldots, (n_1 - 1).$$

Собственное относительно P_1 и P_2 отображение ψ_e называется *неудачным*, если $\deg \psi_e(S_m) < \deg S_m$ для некоторого ненулевого S_m. Заметим, что это определение менее ограничительно, чем определение неудачных отображений вычисления в [20]. Пара образов последовательных субрезультантов S_m и S_{m+1} под действием ψ_e называется *псевдо-gcrd-парой с индексом* m, если $\deg \psi_e(S_m) = m$ и $\psi_e(S_{m+1}) = 0$.

Предложение 4.2. *Пусть P_1, P_2 в $\mathbb{Z}_p[t][x, \delta_p, \sigma_p]$ имеют степени n_1 и n_2 соответственно, $n_1 \geq n_2 > 0$. Пусть G — унитарный gcrd для P_1 и P_2 степени g. Пусть ψ_e — собственное относительно P_1 и P_2 отображение вычисления. Тогда*

(1) *Если ψ_e не неудачно и g положительно, то $(\psi_e(S_g), \psi_e(S_{g-1}))$ — единственная псевдо-gcrd-пара для P_1 и P_2 под действием ψ_e и $\psi_e(G)$ — унитарный многочлен, ассоциированный с $\psi_e(S_g)$.*
(2) *Если ψ_e не неудачно и g нулевое, то у P_1 и P_2 нет псевдо-gcrd-пар и $\phi_e(S_0)$ ненулевой.*
(3) *Если ψ_e неудачно и у P_1, P_2 есть псевдо-gcrd-пара $(\psi_e(S_m), \psi_e(S_{m+1}))$, то $m \geq g$. В этом случае $m = g$, $\psi_e(G)$ — по-прежнему унитарный многочлен, ассоциированный с $\psi_e(S_g)$.*

Доказательство. Первое и второе утверждения следуют из предложения 4.1 и того факта, что ψ_e отображает цепочку субрезультантов P_1 и P_2 с сохранением степени. Последнее же следует из того, что $\mathrm{sres}_{g-1}(P_1, P_2) = \mathrm{sres}_{g-2}(P_1, P_2) = \ldots = \mathrm{sres}_0(P_1, P_2) = 0$. □

Для данных последовательности (9) и собственного относительно P_1 и P_2 отображения вычисления ψ_e мы ищем псевдо-gcrd-пару в последовательности $\psi_e(P_2)$, $\psi_e(S_{n_2-1})$, $\psi_e(S_{n_2-2})$, $\psi_e(S_0)$. Пусть M_{n_2-1} — ассоциированная с S_{n_2-1} матрица. Вычисляем $H_{n_2-1} = \psi_e(S_{n_2-1})$ гауссовым исключением в строках $\psi_e(M_{n_2-1})$. Если $H_{n_2-1} = 0$, то мы получаем псевдо-gcrd-пару $(\psi_e(P_2), H_{n_2-1})$ и возвращаем унитарный многочлен, ассоциированный с $\psi_e(P_2)$. В противном случае полагаем $d = \deg H_{n_2-1}$.

По теореме 4.2 из [19] нам надо вычислить только $H_d = \psi_e(S_d)$. Если степень H_d меньше d, то ψ_e неудачно, выдаём сообщение об ошибке. Иначе мы вычисляем $H_{d-1} = \psi_e(S_{d-1})$ гауссовым исключением в строках матрицы, ассоциированной с $\psi_e(S_{d-1})$. Если $H_{d-1} = 0$, мы получаем псевдо-gcrd-пару (H_d, H_{d-1}) и возвращаем унитарный многочлен, ассоциированный с H_d. Иначе заменяем d на $\deg H_{d-1}$ и повторяем процесс. Если псевдо-gcrd-пар не найдено, мы в конце концов вычислим $H_0 = \psi_e(S_0)$. Если $H_0 \neq 0$, то возвращаем 1 (в этом случае P_1 и P_2 имеют тривиальный gcrd). Иначе сообщаем об ошибке (в этом случае значение e — неудачное).

Описанный выше процесс может выдать либо унитарный многочлен H положительной степени из $\mathbb{Z}_p[x]$, либо 1, либо сообщение об ошибке. В первом случае H — либо образ G под действием ψ_e, либо $\deg H > g$, что означает, что ψ_e неудачно, по предложению 4.2. Во втором случае G тривиален. В последнем случае ψ_e неудачно. Есть не более $n_2^2(n_1 + n_2)n_t$ неудачных отображений вычисления. Так как матрица M_i, ассоциированная с S_i, — подматрица в матрице M_j, ассоциированной с S_j при $i > j$, результаты, полученные при гауссовом исключении в M_i, можно повторно использовать при гауссовом исключении в M_j. Таким образом, сложность вычисления $\psi_e(S_{n_2-1})$, $\psi_e(S_{n_2-2})$, $\ldots$, $\psi_e(S_{g-1})$ та же, что и сложность вычисления $\psi_e(S_{g-1})$ гауссовым исключением. Последняя сложность ограничена выражением $(n_t(n-g)^2 + (n-g)^3)$, в котором $n_t(n-g)^2$ — сложность вычисления $\psi_e(M_{g-1})$, а $(n-g)^3$ — сложность гауссовых исключений в M_{g-1} для дифференциального случая. Использование описанного выше метода вместо GCRD_e дает нам общее улучшение модулярного метода поиска gcrd при g близком к n_2.

Эксперимент 1. Для вычисления gcrd двух данных многочленов Оре p_1 и p_2 реализованы три разных метода: Евклида, без использования дробей и модулярный. Эвристически выбирается один из этих трёх методов на основании догадок о степени $\mathrm{gcrd}(p_1, p_2)$.

Таблица 1 показывает сравнительное время работы в нашем эксперименте [1]. Случайно порождается 10 пар многочленов в дифференциальном кольце. На каждую пару многочленов p_1 и p_2 наложены следующие ограничения:

$$\deg p_1, \deg p_2 \leq 17, \quad \deg \mathrm{gcrd}(p_1, p_2) \geq 2.$$

В таблицу также включено время, потраченное функцией `DEtools[GCRD]`.

Таблица 1. Вычисление gcrd: время (в секундах) для разных методов.

	Евклида	Без дробей	Модулярный	Эвристический	DEtools
1	65.72	27.09	16.57	16.94	33.30
2	184.96	56.11	28.64	29.44	49.85
3	168.88	103.03	31.87	32.10	55.60
4	221.47	166.94	43.09	43.89	70.11
5	25.06	22.58	21.43	22.14	14.94
6	65.61	53.16	33.70	31.92	30.27
7	123.79	79.32	40.87	41.96	37.97
8	148.57	68.68	33.89	35.05	52.83
9	28.71	14.76	15.42	15.63	15.79
10	120.57	85.44	27.54	28.65	59.24

Если $\mathrm{gcrd}(p_1, p_2)$ тривиален, то модулярный метод заметно быстрее, чем любой немодулярный метод, потому что модулярный метод может обнаружить, что p_1 и p_2 взаимно просты, удачным модулярным гомоморфизмом и удачным отображением вычисления. Если $\mathrm{gcrd}(p_1, p_2)$ нетривиален, экспериментальные результаты показывают, что эффективность модулярного метода зависит от следующих факторов:

- сколько делений требуется для вычисления $\mathrm{gcrd}(p_1, p_2)$ в правом алгоритме Евклида;

[1] Все приведённые времена были получены на 400MHz SUN SPARC SOLARIS с 1Gb RAM.

- сколь "прост" $\operatorname{gcrd}(p_1, p_2)$.

Под "простотой" мы подразумеваем, что коэффициенты имеют низкие степени и короткие целые коэффициенты. Чем больше надо делений, тем больше работы проделают немодулярные методы. Чем проще $\operatorname{gcrd}(p_1, p_2)$, тем меньше образов надо для восстановления настоящего gcrd в модулярном методе. При любых входных данных модулярный метод не приводит к разбуханию каких-либо промежуточных выражений.

4.2. **Вычисление lclm.** Применим модулярную технику к вычислению lclm. Пусть $P_1, \ldots, P_m$ из $\mathbb{D}[t][x;\sigma,\delta]$ имеют соответственно положительные степени $d_1, \ldots, d_m$. Пусть $L = \operatorname{lclm}(P_1, \ldots, P_m)$. Чтобы вычислить L, можно сначала вычислить $L_{12} = \operatorname{lclm}(P_1, P_2)$, а затем вычислить $\operatorname{lclm}(L_{12}, P_3, \ldots, P_m)$ рекурсивно (по m). Этот "многошаговый" алгоритм не очень хорошо работает на практике, отчасти потому, что коэффициенты промежуточных lclm обычно гораздо сложнее, чем у P_i.

Процедура *LCLM* в Maple-пакете `DEtools`, написанная ван Хоие, даёт прямой метод вычисления lclm нескольких многочленов Оре. Этот метод работает следующим образом. Пусть

$$d = d_1 + \cdots + d_m \quad \text{и} \quad Q_d = q_d x^d + \cdots + q_0,$$

где $q_0, \ldots, q_d$ — произвольные коэффициенты. Для $i = 1, \ldots, m$ вычисляется правый остаток R_i от деления Q_d на P_i. Ясно, что Q_d — общее левое кратное $P_1, \ldots, P_m$ степени не выше d, если и только если $R_1 = \cdots = R_m = 0$. Это приводит к линейной однородной алгебраической системе

$$(q_0, \ldots, q_d) M_d = 0, \tag{10}$$

где M — $((d+1) \times d)$-матрица над k. Для удобства мы будем говорить, что

$$\tilde{Q}_d = \tilde{q}_d x^d + \cdots + \tilde{q}_0$$

из $\mathbb{D}[t][x;\sigma,\delta]$ — решение (10), если $(\tilde{q}_0, \ldots, \tilde{q}_d)$ — решение системы (10); таким образом, L — ненулевое решение (10) наименьшей степени.

Итак, чтобы найти L, надо найти решение (10) наименьшей степени ($\deg L$ может быть меньше d).

Предложение 4.3. *Значение* $\deg L$ *равно рангу* M_d *из (10).*

Доказательство. Пусть $\deg L = l$. Поскольку $l \leq d$, все L, xL, ..., $x^{d-l}L$ являются решениями (10). Итак, пространство решений (10) имеет размерность не меньше $(d+1-l)$. С другой стороны, любое ненулевое решение $\tilde{Q}_d$ уравнения (10) — общее левое кратное $P_1, \ldots, P_m$ степени не выше d, так что правый остаток от деления $\tilde{Q}_d$ на L равен нулю, то есть $\tilde{Q}$ — k-линейная комбинация L, $xL, \ldots, x^{d-l}L$. Значит, пространство решений (10) имеет размерность $(d+1-l)$. Следовательно, ранг M_d равен d. □

Для вычисления L мы, во-первых, строим матрицу M_d, заданную (10). Во-вторых, применяем модулярное отображение и отображение вычисления к элементам M_d, чтобы получить матрицу M'_d над $\mathbb{Z}_p$. В-третьих, вычисляем ранг r для M'_d. В-четвёртых, полагаем

$$Q_r = q_r x^r + \cdots + q_0,$$

где $q_0, \ldots, q_r$ — неопределённые коэффициенты. Для $i = 1, \ldots, m$ вычисляем правый остаток R_i от деления Q_r на P_i. Условие $R_1 = \cdots = R_m = 0$ даёт линейную однородную алгебраическую систему

$$(q_0, \ldots, q_r)M_r = 0. \tag{11}$$

Любое нетривиальное решение (11) соответствует $\mathrm{lclm}(P_1, \ldots, P_m)$, потому что $r \leq \deg L$ по предложению 4.3. Если (11) имеет только тривиальное решение, то заменяем r на $(r+1)$ и повторяем четвёртый шаг. Так как r почти всегда равно рангу M_d, то на практике, скорее всего, не возникнет необходимости повторения четвёртого шага. Мы будем ссылаться на этот метод как на "одношаговый" метод.

Эксперимент 2. Множество испытаний, связанных с вычислением lclm, состоит из 10 троек многочленов в дифференциальном кольце. На каждую тройку многочленов p_1, p_2 и p_3 мы накладываем следующие ограничения:

$$\deg p_1 = \deg p_2 = 5,\ \deg \mathrm{gcrd}(p_1, p_2) = 2,\ \deg p_3 = 3.$$

Таблица 2 показывает сравнение времени работы многошагового и одношагового метода. Мы также включаем время для функции `DEtools[LCLM]`.

Заметим, что если $\deg \operatorname{lclm}(p_1, p_2, p_3) = \deg p_1 + \deg p_2 + \deg p_3$, то время для одношагового метода и `DEtools[LCLM]` примерно одинаково.

Таблица 2. Вычисление lclm: время (в секундах) для разных методов.

	Многошаговый	Одношаговый	DEtools
1	114.53	25.99	87.48
2	147.36	24.28	107.60
3	111.95	33.36	105.33
4	124.15	30.41	84.41
5	128.65	30.76	102.63
6	144.56	29.35	103.03
7	96.84	18.60	61.73
8	115.08	28.36	92.74
9	140.59	21.18	122.81
10	123.97	16.13	62.31

Мы завершаем этот раздел рассмотрением вычислений lclm в прямом алгоритме вычисления минимального телескопирующего оператора для рациональной функции [18]. Рассмотрим рациональную функцию $R(n,k) = R_1 + R_2 + R_3$, где

$$\begin{aligned} R_1 &= \frac{n+1}{(2\,n+5\,k+3)^2} + \frac{n}{(2\,n+5\,k+5)^2}, \\ R_2 &= \frac{n+2}{3\,n+4\,k+4} - \frac{3}{3\,n+4\,k-2}, \\ R_3 &= \frac{(n-3)^2}{n-7\,k+5} + \frac{1}{n-7\,k+6}. \end{aligned}$$

Вычисленные минимальные телескопирующие операторы L_1 для R_1, L_2 для R_2 и L_3 для R_3 равны

$$\begin{aligned}
L_1 &= \mathrm{OrePoly}\left((n+5)(n+4)(n+3)(n+2)(2n+7),\, 5\,(n+5)(n+4)(n+3),\right.\\
&\quad -5\,(n+5)(n+4)(n+1),\, 5\,(n+5)(n+2)(n+1),\\
&\quad \left.-5\,(n+3)(n+2)(n+1),\, -(2n+5)(n+4)(n+3)(n+2)(n+1)\right),\\
L_2 &= \mathrm{OrePoly}\left(-n^2-10n-15,\, 0,\, -12,\, 0,\, n^2+6n-1\right),\\
L_3 &= \mathrm{OrePoly}\left(n^{14}+14\,n^{13}+63\,n^{12}+28\,n^{11}-553\,n^{10}-1218\,n^9+929\,n^8+\right.\\
&\quad 4984\,n^7+1848\,n^6-6496\,n^5-4592\,n^4+2688\,n^3+2304\,n^2+1,\\
&\quad -7\,(2\,n+1)\,(n-1)^2\,(n+3)^2\,(n+2)^2\,(n+1)^2\,n^2,\, 7\,(2\,n+1)\,(n+3)^2\\
&\quad (n+2)^2\,(n+1)^2\,n^2,\, -7\,(2\,n+1)\,(n+3)^2\,(n+2)^2\,(n+1)^2\,,\\
&\quad 7\,(2\,n+1)\,(n+3)^2\,(n+2)^2\,,\, -7\,(2\,n+1)\,(n+3)^2\,,\, 14\,n+7,\\
&\quad \left.-n^{14}+28\,n^{12}-294\,n^{10}+1444\,n^8-3409\,n^6+3528\,n^4-1296\,n^2-1\right)
\end{aligned}$$

(о представлении многочленов Оре см. раздел 5.2). Минимальный телескопирующий оператор L для рациональной функции R равен $\mathrm{lclm}(L_1, L_2, L_3)$. Если воспользоваться одношаговым методом, то это вычисление L займёт 6.28 сек., использование многошагового метода потребует 273.90 сек.

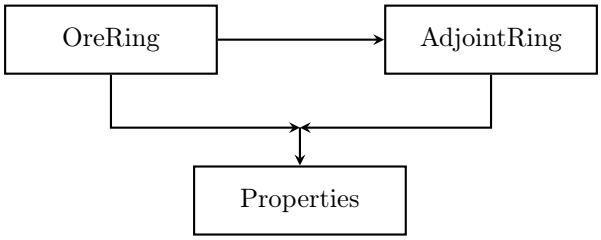
5. Пакет `OreTools`

Основная цель пакета `OreTools` — предоставить простейшие операции в заданном кольце Оре и упростить дальнейшую разработку алгоритмов различных вычислений в кольцах Оре. Пакет интегрирован в Maple. В частности, он используется (а) как основа пакета `LinearOperators`, включающего функции вычисления минимальных полностью факторизуемых аннуляторов [5], и для вычисления даламберовых решений неоднородных линейных функциональных уравнений [6]; (б) в пакете `SumTools` [2] для эффективного прямого вычисления минимальных Z-пар рациональных функций [18], для вычисления бесконечных сумм методом аккуратного интегрирования и (в) в пакете `Slode` [29] для нахождения формальных решений линейных однородных дифференциальных уравнений в виде рядов с даламберовыми коэффициентами.

В этом разделе мы даём обзор пакета `OreTools`. Детальное обсуждение предлагаемых возможностей и детали реализации см. в [4]. Ранняя версия пакета `OreTools` описывалась в [5, Разд. 6]. Код этой версии был разработан Е.В.Зимой.

5.1. **Определение кольца Оре и сопряжённого к нему; работа с параметрами этих колец.** На рисунке 1 представлено множество функций, которые помогают определить кольцо Оре и кольцо, сопряжённое к данному кольцу Оре (которое само является кольцом Оре), а также функции для работы с параметрами кольца Оре.

Рис. 1. Определение кольца Оре и работа с его параметрами



Кольцо Оре от одной переменной определяется посредством функции *SetOreRing*. Предопределены *дифференциальное* кольцо, кольцо со *сдвигом* и с *q-сдвигом*. Чтобы определить другие кольца, нужно задать процедуры вычисления σ, δ, $\theta(1)$ и σ^{-1}.

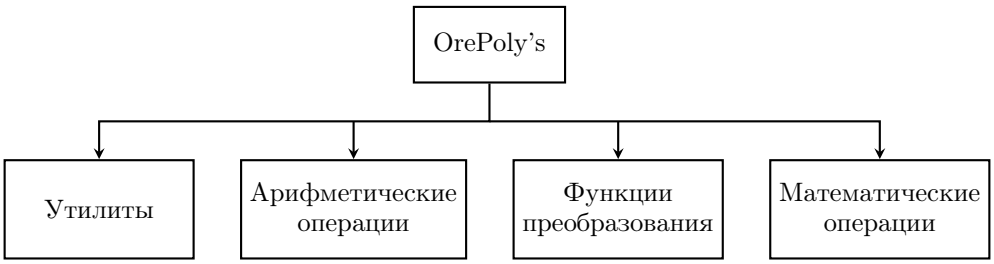
Сопряжённое к данному кольцу Оре определяется функцией *AdjointRing*. Её вход — кольцо Оре, а выход — сопряжённое к нему.

Со свойствами данного кольца Оре, напр., $\sigma, \sigma^{-1}, \theta(1), \delta$, можно работать в подмодуле `Properties`.

5.2. **Средства работы с многочленами Оре.** Многочлен Оре представляется структурой OrePoly. Она состоит из ключевого слова OrePoly с последовательностью коэффициентов, начинающейся со степени нуль. Например, в дифференциальном случае с дифференциальным оператором D OrePoly$(2/t, t, t+1, 1)$ представляет оператор $2/t + t\,D + (t+1)\,D^2 + D^3$.

На рисунке 2 представлены основные средства работы с многочленами Оре. Их можно разделить на четыре группы: утилиты, арифметические операции, функции преобразования и математические операции.

Рис. 2. Средства работы с многочленами Оре



Утилиты включают функции для таких действий с многочленами Оре, как, напр., нахождение старшего и младшего коэффициентов или степени данного многочлена Оре.

Основные арифметические операции над многочленами Оре включают

(1) линейные операции: сложение, вычитание, умножение на скаляр;
(2) операции по нормализации: вычисление содержания, примитивной части, левого и правого унитарных ассоциированных;
(3) умножение, деления (левые и правые остатки и частные);
(4) левый и правый gcd, lcm, расширенный gcd и gcrd, зависящий от параметра [13].

Функции преобразования играют роль интерфейса между пакетом `OreTools` и системой Maple. Они включают в себя функции прямого и обратного преобразования между данным многочленом Оре и соответствующим линейным функциональным уравнением.

Пакет поддерживает некоторые математические операции. Они включают в себя функции аккуратного интегрирования (раздел 3.3) и вычисления интегрирующего множителя (раздел 3.2).

Подмодуль `Modular` предоставляет пользователям основные операции над многочленами Оре, коэффициенты которых — рациональные функции над $\mathbb{Z}_p$;

а подмодуль `FractionFree` предоставляет пользователям операции без использования дробей над многочленами Ope, коэффициенты которых — многочлены над $\mathbb{Z}$.

5.3. **Примеры.** В кольце A со сдвигом

```
> A := SetOreRing(n,'shift');
```

$$A := \text{UnivariateOreRing}(n, \mathit{shift})$$

рассмотрим два многочлена Ope p_1 и p_2:

```
> p_1 := \OrePoly((n-3)*n^2,n^4+n^3-4*n^2-n-2,
  n^4+3*n^3+2*n^2+n-4,n^3+6*n^2+10*n+2,n^2+6*n+6):
> p_2 := \OrePoly((n-3)*n^3,n^5+n^4-6*n^3+4*n^2-3*n-2,
  n^5+n^4-n^3+7*n^2-2*n-3,n^4+5*n^3+7*n^2+5*n+1,(n^2+6*n+6)*n):
```

Вычислим gcrd p_1 и p_2:

```
> GCD['right'](p_1,p_2,A);
```

$$\text{OrePoly}\left(\frac{n-3}{n^2-3}, 1\right).$$

Вычислим gcld p_1 и p_2:

```
> GCD['left'](p_1,p_2,A);
```

$$\text{OrePoly}\left(n^2, n+1, 1\right).$$

Для двух многочленов Ope p_3 и p_4

```
> p_3 := \OrePoly(1,1,0,(a+2)*n):
> p_4 := \OrePoly(0,(a+2)*(a+1)*n):
```

предположим заранее, что значение параметра a удовлетворяет уравнению $a(a+1)(a+2) = 0$, и вычислим gcrd p_3 и p_4 в зависимости от параметра a:

```
> ParametricGCRD(p_3, p_4, (a+1)*(a+2)*a, a, A);
```

$$\begin{cases} \text{OrePoly}\,(-1) & a = 0, \\ \text{OrePoly}\,(1, 1, 0, n) & a + 1 = 0, \\ \text{OrePoly}\,(1, 1) & a + 2 = 0. \end{cases}$$

6. Сравнение

Есть и другие Maple-пакеты, которые предоставляют средства для работы с общими кольцами Ope или с конкретным кольцом Ope. Среди них пакет `Ore_algebra` [9] для колец Ope от нескольких переменных, пакет `DEtools` для дифференциального случая, пакет `LREtools` для случая сдвига и пакет `QDifferenceEquations` для случая q-сдвига. Хотя основное внимание `LREtools` и `QDifferenceEquations` сосредоточено на поиске решений специального вида (напр., полиномиальных, рациональных) для линейных рекуррентных (q-рекуррентных) соотношений с полиномиальными коэффициентами, пакеты `Ore_algebra` и `DEtools` предоставляют, хотя и в меньшей степени по сравнению с пакетом `OreTools`, поддержку основных операций в кольцах Ope.

Сравнение `DEtools` с `OreTools` проведено в двух экспериментах, описанных в разделе 4. В настоящем разделе мы сравниваем `Ore_algebra` с `OreTools`.

Единственная функциональность пакетов, которая позволяет провести прямое сравнение между `Ore_algebra` и `OreTools`, — это расширенный правый алгоритм Евклида: *skew_ gcdex* в `Ore_algebra` и *ExtendedGCD* в `OreTools`. Использование *skew_ gcdex* является единственным способом вычислить gcrd в пакете `Ore_algebra` (неизбежное построение двух дополнительных многочленов иногда оказывается избыточным).

В этом эксперименте использованы два набора тестов. Каждый набор состоит из 10 пар многочленов p_1 и p_2. Пары первого набора порождались в кольце со сдвигом, а второго — в дифференциальном кольце.

На каждую пару p_1, p_2 наложены следующие ограничения:

$$7 \le \deg p_1,\ \deg p_2 \le 10; \quad \deg \operatorname{gcrd}(p_1, p_2) \ge 2;$$

Каждый коэффициент p_1 и p_2 — многочлен степени не более 5 и состоит не более чем из 2 членов.

Таблицы 3 и 4 отражают затраты *ExtendedGCD* и *skew_ gcdex* по времени (в секундах) и памяти (в килобайтах).

Таблица 3. OreTools и Ore_algebra: рекуррентный случай.

	ExtendedGCD		skew_gcdex	
	время	память	время	память
1	123	703,329	1,691	4,669,006
2	55	276,828	487	1,555,668
3	183	830,378	1,269	3,420,360
4	44	230,488	648	1,977,186
5	145	654,363	364	1,219,685
6	113	511,026	268	979,230
7	47	236,447	470	1,549,453
8	179	780,795	656	1,984,256
9	49	241,977	128	490,365
10	89	417,157	177	635,439

Таблица 4. OreTools и Ore_algebra: дифференциальный случай.

	ExtendedGCD		skew_gcdex	
	время	память	время	память
1	24	245,039	765	2,828,435
2	20	169,934	189	976,940
3	38	340,290	437	1,968,124
4	20	167,486	300	1,324,531
5	11	81,216	151	861,778
6	23	206,490	53	360,019
7	17	159,388	216	1,030,755
8	23	201,707	333	1,370,342
9	13	113,148	47	319,017
10	13	117,665	61	418,924

Стоит заметить, что все кольца Ope, объявленные в пакете `Ore_algebra`, по умолчанию имеют целые коэффициенты, и любой другой тип коэффициентов надо явно объявлять. Поэтому простейшие операции могут потребовать от пользователей нетривиальных усилий и знаний.

7. Доступ

Информация о доступе к библиотечному архиву пакета `OreTools`, образцам рабочих распечаток Maple, а также об установке пакета находится по следующему адресу:

`http://www.scg.math.uwaterloo.ca/~hqle/code/OreTools/OreTools.html`

Список литературы

[1] С.А.Абрамов. Рациональные решения линейных обыкновенных дифференциальных и разностных уравнений с полиномиальными коэффициентами. *Журнал вычисл. матем. и матем. физики*, 1989, No 11, С. 1611–1620.

[2] S.A. Abramov, J.C. Carette, K.O. Geddes, H.Q. Le. *Symbolic Summation in Maple*. Technical Report CS-2002-32, School of Computer Science, University of Waterloo, Ontario, Canada, 2002.

[3] S.A. Abramov, M. van Hoeij. Integration of solutions of linear functional equations. *Integral Transformations and Special Functions* **8** (1999) no. 1-2, 3–12.

[4] S.A. Abramov, H.Q. Le, Ziming Li. `OreTools`: a computer algebra library for univariate Ore polynomial rings. *Technical Report CS-2003-12*, School of Computer Science, University of Waterloo, Ontario, Canada.

[5] S.A. Abramov, E.V. Zima. Minimal completely factorable annihilators. In: W. Küchlin (ed.), *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ACM Press, 290–297.

[6] S.A. Abramov, E.V. Zima. D'Alembertian solutions of inhomogeneous linear equations (differential, difference, and some other). In: Y.N. Lakshman (ed.), *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, ACM Press, 232–240.

[7] S.A. Abramov, E.V. Zima. A universal program to uncouple linear systems. In: *Proceedings of International Conference on Computational Modeling and Computing in Physics*, Dubna, Russia, Sept. 16-21, 1996 (1997) 16–26.

[8] M. Bronstein, M. Petkovšek. An introduction to pseudo–linear algebra, *Theoretical Computer Science* **157** (1996) 3–33.

[9] F. Chyzak, B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *Journal of Symbolic Computation* **26** (1998) no. 2, 187–227.

[10] P.M. Cohn. *Free Rings and Their Relations*. Academic Press, 1971.

[11] P.M. Cohn. *Skew Fields, Theory of General Division Rings*. Encyclopedia of Mathematics and its applications **57** (1995) Cambridge University press.

[12] M. Giesbrecht, Y. Zhang. Factoring and decomposing Ore polynomials over $\mathbb{F}_p(t)$. To appear in the *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*.

[13] П.Е.Глотов. Алгоритм поиска наибольшего общего делителя полиномов Оре с полиномиальными коэффициентами, зависящими от параметра. *Программирование.* 1998. N 6. С. 14–21.

[14] R.W. Gosper. Decision procedure for indefinite hypergeometric summation. *Proc. Natl. Acad. Sci. USA* **75** (1978) 40–42.

[15] J. van der Hoeven. FFT-like multiplication of linear differential operators. *Journal of Symbolic Computation* **33** (2002) no. 1, 123 - 127.

[16] N. Jacobson. Pseudo-linear transformations. *Annals of Mathematics* **38** (1937) no. 2, 484–507.

[17] E. Landau. Über irreduzible Differentialgleichungen. *J. für die reine und angewandte Mathematik* **124** (1902) 115–120.

[18] H.Q. Le. A direct algorithm to construct the minimal Z-pairs for rational functions. *Advances in Applied Mathematics* **30** (2003) 137–159.

[19] Z. Li. A subresultant theory for ore polynomials with applications. In: O. Gloor (ed), *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, ACM Press, 132–139.

[20] Z. Li, I. Nemes. A modular algorithm for computing greatest common right divisors of Ore polynomials. In: W. Küchlin (ed.), *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ACM Press, 282–289.

[21] A. Loewy. Über reduzible lineare homogene Differentialgleichungen. *Math. Annalen* **56** (1903) 549–584.

[22] A. Loewy. Über vollstandig reduzible lineare homogene Differentialgleichungen. *Math. Annalen* **62** (1906) 89–117.

[23] M.B. Monagan, K.O. Geddes, K.M. Heal, G. Labahn, S.M. Vorkoetter, J. McCarron, P. DeMarco. *Maple 8 Introductory Programming Guide*. Waterloo Maple Inc., Waterloo, Ontario, Canada, 2002.

[24] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics* **34** (1933) 480–508.

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

[26] O. Ore. Formale Theorie der linearen Differentialgleichungen (Zweiter Teil). *J. für die reine und angewandte Mathematik* **1** (1932), 233–252.

[27] E. G. C. Poole. *Introduction to the theory of linear ordinary differential equations*. Dover Publications Inc., New York, 1936.

[28] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation* **14** (1992) 243–264.

[29] Рябенко А.А. Maple-пакет символьного построения решений линейных обыкновенных дифференциальных уравнений в виде степенных рядов *Программирование*. 1999. N 5. С. 71–80.

[30] J.H.M. Wedderburn. Non-commutative domains of integrity. *J. Reine Angew. Math.* **167** (1932) 129–141.

Вычислительный центр им. Дородницына, Российская академия наук, Москва, Россия

E-mail address: abramov@ccas.ru

Symbolic Computation Group, University of Waterloo, Waterloo, Canada

E-mail address: hqle.@scg.math.uwaterloo.ca

Symbolic Computation Group, University of Waterloo, Waterloo, Canada

E-mail address: z6li@scg.math.uwaterloo.ca