Стандартные базисы, согласованные с нормированием, и вычисления в идеалах и полилинейных рекуррентах

Е. В. ГОРБАТОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: lofar@mail.ru

УДК 512.714+519.725

Ключевые слова: согласованный стандартный базис, каноническая система образующих, схема симплификации, полилинейная рекуррентная последовательность, полилинейный регистр сдвига, цилиндрический идеал.

Аннотация

В работе продолжено начатое А. А. Нечаевым, Д. А. Михайловым и автором исследование согласованных с нормированием стандартных базисов идеалов кольца полиномов $R[X] = R[x_1, \ldots, x_k]$ над коммутативным артиновым цепным кольцом R. Введены новые, основанные на координатном разложении элементов из R, порядок на одночленах и алгоритм редуцирования полинома полиномом; доказано, что всякий идеал имеет единственный редуцированный, в смысле этого алгоритма, стандартный базис. Решены некоторые классические вычислительные задачи: построение системы представителей классов вычетов, нахождение порождающих модуля сизигий, вычисление частных и пересечений идеалов, задача элиминации. Построен алгоритм проверки цикличности ЛРП-семейства $L_R(I)$, обобщающий ранее известные результаты на случай многих переменных. Найдены новые условия, определяющие, когда данные диаграмма Ферре $\mathcal{F}$ и полная система $\mathcal{F}$-унитарных полиномов образуют регистр сдвига; на основании этих результатов построен алгоритм поднятия редуцированного базиса Грёбнера унитарного идеала до стандартного базиса той же мощности.

Abstract

E. V. Gorbatov, Standard bases concordant with the norm and computations in ideals and polylinear recurring sequences, Fundamentalnaya i prikladnaya matematika, vol. 10 (2004), no. 3, pp. 23—71.

Standard bases of ideals of the polynomial ring $R[X] = R[x_1, \ldots, x_k]$ over a commutative Artinian chain ring R that are concordant with the norm on R have been investigated by D. A. Mikhailov, A. A. Nechaev, and the author. In this paper we continue this investigation. We introduce a new order on terms and a new reduction algorithm, using the coordinate decomposition of elements from R. We prove that any ideal has a unique reduced (in terms of this algorithm) standard basis. We solve some classical computational problems: the construction of a set of coset representatives, the finding of a set of generators of the syzygy module, the evaluation of ideal quotients and intersections, and the elimination problem. We construct an algorithm testing the cyclicity of an LRS-family $L_R(I)$, which is a generalization of known results to the multivariate case. We present new conditions determining whether a Ferre diagram $\mathcal{F}$ and a full system of

Фундаментальная и прикладная математика, 2004, том 10, № 3, с. 23—71.

$\mathcal{F}$-monic polynomials form a shift register. On the basis of these results, we construct an algorithm for lifting a reduced Gröbner basis of a monic ideal to a standard basis with the same cardinality.

Введение

Развитие прикладных аспектов современной алгебры в последние десятилетия связано в значительной степени с построением основ теории полилинейных рекуррентных последовательностей и теории линейных кодов над конечными модулями и их приложениями. Возникающие при этом задачи вычислительного характера чаще всего сводятся к необходимости оперирования с полиномиальными идеалами над конечными кольцами.

Для решения этих задач можно использовать технику стандартных базисов полиномиальных идеалов, общая теория которых в настоящее время хорошо развита [5,12]. Однако попытки использовать стандартные базисы, которые строятся по известным общим алгоритмам, показали, что эти базисы малоэффективны. Дальнейшие исследования выявили, что для решения поставленных задач нужно строить базисы идеалов по специально разработанным алгоритмам, учитывающим специфику кольца коэффициентов R [2,7,9,10].

В данной работе рассматривается случай, когда R — коммутативное конечно цепное кольцо (наиболее востребованный с точки зрения практических приложений). Алгоритмы построения стандартных базисов идеалов кольца $R[X]$ основаны на некотором линейном и согласованном с умножением упорядочении мономов $rx_1^{i_1}\dots x_k^{i_k}$ этого кольца. При этом упомянутые выше общие алгоритмы используют лишь порядки, однозначно определяемые набором показателей $i_1,\dots,i_k$, и не учитывают специфику коэффициента r. Стандартные базисы, которые строятся в данной работе, наоборот, основаны на упорядочениях мономов, которые в первую очередь учитывают эту специфику: место идеала rR в конечной цепи идеалов кольца R.

Идея использования таких порядков для построения стандартных базисов с целью решения названных выше прикладных задач была впервые реализована А. А. Нечаевым в [7] для кольца многочленов от одного переменного и затем развивалась в [2,9,10].

В классическом случае кольца полиномов над полем одной из важнейших характеризаций стандартного базиса (базиса Грёбнера) является единственность нормальной формы полинома при редуцировании. Стандартные базисы из [2,7,9,10] не обладают этим свойством. В данной работе введены новые, основанные на координатном разложении элементов из R (см. предложение 1.16), порядок на одночленах и алгоритм редуцирования. Доказано (см. теорему 1.44), что система полиномов χ является стандартным базисом, если и только если всякий полином из $R[X]$ обладает единственной нормальной формой при таком редуцировании относительно χ. Данное утверждение позволило построить систему представителей классов вычетов по модулю некоторого полиномиального

идеала (см. предложение 2.1) и обобщить формулу для мощности фактор-кольца из [17] (см. следствие 2.3). Доказано, что, как и в классическом случае, всякий идеал имеет единственный редуцированный, в смысле этого алгоритма, стандартный базис (см. теорему 1.61).

В данной работе построены алгоритмы, решающие классические вычислительные задачи в кольце полиномов $R[X]$, такие как: нахождение порождающих модуля сизигий, вычисление частных и пересечений идеалов, задача элиминации (см. разделы 2.2 и 2.3). Эти алгоритмы позволили описать процедуру проверки цикличности семейства линейных рекуррентных последовательностей $L_R(I)$, что является обобщением результатов из [19] на случай многих переменных (см. раздел 3.1).

Найдены новые условия, определяющие, когда данные диаграмма Ферре $\mathcal{F}$ и полная система $\mathcal{F}$-унитарных полиномов χ образуют регистр сдвига (см. теорему 3.9). Эти условия даны в терминах коэффициентов полиномов из χ и представляют, таким образом, решение одной из сформулированных в [18] задач. С использованием этого результата, а также методов решения систем нелинейных алгебраических уравнений над кольцами Галуа из [10], в работе для случая, когда R — кольцо Галуа, построена эффективная процедура проверки существования (и нахождения при положительном ответе) поднятия данного базиса Грёбнера над $\bar{R} = R/\operatorname{rad}(R)$ до стандартного базиса над R с сохранением мощности (см. раздел 3.3).

1. Схемы симплификации и стандартные базисы

1.1. Порядки на полиномах

При построении теории стандартных базисов важную роль играют упорядочения мономов, одночленов и полиномов. В данном разделе мы с общих позиций изучаем эти порядки.

Ввиду неоднозначности терминологии, введём определения и обозначения используемых понятий и объектов.

Мы работаем с множеством натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$, множеством натуральных чисел с нулём $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, отрезками целых чисел $\overline{m,n} = \{i \in \mathbb{Z} \mid m \leqslant i \leqslant n\}$.

Мы говорим, что бинарное отношение $\preceq$ на M задаёт *порядок* на M или что $(M, \preceq)$ является *упорядоченным* множеством, если это отношение рефлексивно, транзитивно и антисимметрично (в этом случае также употребляют термин *частично упорядоченное множество*). Если любые два элемента из M сравнимы относительно порядка $\preceq$, мы говорим, что $(M, \preceq)$ — *линейно упорядоченное* множество, а порядок $\preceq$ называем *линейным*. Наконец, линейный порядок $\preceq$, удовлетворяющий условию минимальности (т. е. условию обрыва убывающих цепочек), называем *полным* и при таком условии говорим, что $(M, \preceq)$ — *вполне упорядоченное* множество.

Зафиксируем множество переменных $X = \{x_1, \dots, x_k\}$, $k \geqslant 1$. Пусть $[X] = [x_1, \dots, x_k]$ — полугруппа коммутативных мономов над X. Пусть также R — некоторое коммутативное кольцо с единицей. *Полугруппой одночленов* назовём подполугруппу

$$[R, X] = \{au \mid a \in R,\ u \in [X]\}$$

полугруппы $(R[X], \cdot)$. Порядок $\preceq$ на $[R, X]$ назовём *разделяющим мономы*, если для любых $a, b \in R \setminus 0$ и $u, v \in [X]$, $u \neq v$,

$$au \prec bv \quad \text{или} \quad bv \prec au.$$

(Мы всегда полагаем, что вместе с порядком $\preceq$ заданы и порядки $\succeq$, $\prec$, $\succ$, при этом, например, $a \prec b \iff (a \preceq b) \wedge (a \neq b)$.) При заданном разделяющем мономы порядке $\preceq$ на $[R, X]$ всякий ненулевой полином $F \in R[X]$ можно представить в виде

$$F = a_1u_1 + a_2u_2 + \ldots + a_nu_n, \tag{1.1}$$

где $a_i \in R \setminus 0$, мономы u_i попарно различны и $a_1u_1 \succ a_2u_2 \succ \ldots \succ a_nu_n$. В таком случае *ведущий член* полинома F *относительно порядка* $\preceq$ определим как

$$\mathrm{lt}_{\preceq}(F) = a_1u_1.$$

Также считаем, что $\mathrm{lt}_{\preceq}(0) = 0$.

Предложение 1.1. *Пусть $\preceq$ — разделяющий мономы порядок на $[R, X]$, тогда эквивалентны следующие условия*:

1) *для любых $F \in R[X]$ и $U \in [R, X]$*

$$\mathrm{lt}_{\preceq}(FU) = \mathrm{lt}_{\preceq}(F)U;$$

2) *для любых элементов $a, b, c \in R$ и мономов $u, v, w \in [X]$*

$$\left.\begin{array}{l} au \prec bv, \\ u \neq v, \\ ac \neq 0,\ bc \neq 0 \end{array}\right| \implies acuw \prec bcvw \tag{1.2}$$

и

$$\left.\begin{array}{l} au \prec bv,\ bc = 0, \\ u \neq v \\ a \neq 0,\ b \neq 0 \end{array}\right| \implies ac = 0. \tag{1.3}$$

Доказательство. Докажем импликацию 1) $\implies$ 2). Пусть в (1.2) выполнены все посылки. Положим $U = cw$ и $F = au + bv$, тогда согласно 1) $\mathrm{lt}_{\preceq}(acuw + bcvw) = bcvw$ и, значит, поскольку порядок $\preceq$ разделяет мономы, $acuw \prec bcvw$.

Докажем (1.3). Пусть $U = c$ и $F = au + bv$, тогда ввиду 1) справедливо $\mathrm{lt}_{\preceq}(acu) = bcv = 0$ и, значит, $ac = 0$.

Проверим импликацию 2) $\Longrightarrow$ 1). Если $F = 0$ или $U = bv = 0$, то условие из 1) очевидно выполнено. Пусть $F \neq 0$ и $U \neq 0$. Представим F в виде (1.1). Если $a_1 b = 0$, то согласно (1.3) $FU = 0$, и утверждение доказано. Пусть $a_1 b \neq 0$, тогда ввиду (1.2) $\mathrm{lt}_{\preceq}(FU) = a_1 b u_1 v = \mathrm{lt}_{\preceq}(F)U$. □

Разделяющий мономы порядок $\preceq$ на $[R, X]$, удовлетворяющий равносильным условиям 1) и 2) из предложения 1.1, назовём *мультипликативным*.

Представляет интерес описание класса колец R, для которых существует мультипликативный порядок на $[R, X]$. С этой целью введём некоторые определения.

Пусть R — коммутативное кольцо, определим на нём отношение $\lesssim_{\mathrm{An}}$, а именно для любых $a, b \in R$ положим[1]

$$a \lesssim_{\mathrm{An}} b \iff \mathrm{An}(b) \subseteq \mathrm{An}(a).$$

Легко видеть, что отношение $\lesssim_{\mathrm{An}}$ рефлексивно и транзитивно, то есть является отношением предпорядка на R. Как и всякий предпорядок, отношение $\lesssim_{\mathrm{An}}$ индуцирует отношение эквивалентности $\sim_{\mathrm{An}}$ и порядок $<_{\mathrm{An}}$ на R:

$$a \sim_{\mathrm{An}} b \iff (a \lesssim_{\mathrm{An}} b) \wedge (b \lesssim_{\mathrm{An}} a) \iff \mathrm{An}(b) = \mathrm{An}(a),$$
$$a <_{\mathrm{An}} b \iff (a \lesssim_{\mathrm{An}} b) \wedge (a \not\sim_{\mathrm{An}} b) \iff \mathrm{An}(b) \subsetneq \mathrm{An}(a).$$

Ясно, что 0 является наименьшим элементом, а всякий не делитель нуля — максимальным элементом относительно порядка $<_{\mathrm{An}}$.

Определение 1.2. Пусть $(U, \cdot)$ — полугруппа и $\preceq$ — порядок на U. Тройка $(U, \cdot, \preceq)$ называется *упорядоченной полугруппой*, если

$$(a \preceq b) \implies (ac \preceq bc) \wedge (ca \preceq cb)$$

для любых $a, b, c \in U$. Если $\preceq$ — линейный (полный) порядок на U, то говорят, что $(U, \cdot, \preceq)$ — *линейно* (*вполне*) *упорядоченная полугруппа*.

Предложение 1.3. *Пусть R — коммутативное кольцо, тогда:*

1) *если на $[R, X]$ существует мультипликативный порядок, то предпорядок $\lesssim_{\mathrm{An}}$ линеен, то есть для любых $a, b \in R$ или $a \lesssim_{\mathrm{An}} b$, или $b \lesssim_{\mathrm{An}} a$, иными словами, аннуляторы элементов из R образуют цепь в решётке идеалов R;*
2) *если предпорядок $\lesssim_{\mathrm{An}}$ линеен и для любых $a, b, c \in R$*

$$(a <_{\mathrm{An}} b) \wedge (bc \neq 0) \implies ac <_{\mathrm{An}} bc, \tag{1.4}$$

то для всякого порядка $\preceq$ на $[X]$, такого что $([X], \preceq)$ — линейно упорядоченная полугруппа, соотношение

$$au \prec bv \overset{\text{def}}{\iff} \begin{cases} a <_{\mathrm{An}} b \ \ \textit{или} \\ a \sim_{\mathrm{An}} b, \ a \neq 0 \textit{и} u \prec v \end{cases} \tag{1.5}$$

определяет мультипликативный порядок на $[R, X]$.

[1] Для $\chi \subseteq R$ идеал $\mathrm{An}(\chi) = \{s \in R \mid \chi s = 0\}$ называется *аннулятором* χ.

Доказательство. Докажем первое утверждение. Пусть на $[R, X]$ имеется некоторый мультипликативный порядок $\preceq$. Возьмём любые $a, b \in R \setminus 0$ и рассмотрим одночлены a и bx_1. Поскольку $1 \neq x_1$ и порядок $\preceq$ разделяет мономы, мы будем иметь или $a \prec bx_1$, или $bx_1 \prec a$. Согласно (1.3) или $\mathrm{An}(b) \subseteq \mathrm{An}(a)$, или $\mathrm{An}(a) \subseteq \mathrm{An}(b)$. Если a или b равно 0, то утверждение очевидно, поскольку $\mathrm{An}(0) = R$.

Докажем второе утверждение. Очевидно, что формула (1.5) задаёт разделяющий мономы порядок на $[R, X]$. Ясно также, что для этого порядка имеет место условие (1.3). Проверим, что выполняется соотношение (1.2).

Пусть выполняются все посылки из (1.2). Если $a <_{\mathrm{An}} b$, то в силу (1.4) $ac <_{\mathrm{An}} bc$. Если $a \sim_{\mathrm{An}} b$, то $u \prec v$ и $ac \sim_{\mathrm{An}} bc$. В любом случае $acuw \prec bcvw$. □

Пусть R — коммутативное артиново кольцо. Модуль Q_R называется *квазифробениусовым* модулем (*QF-модулем*), если для любых идеала $I \lhd R$ и подмодуля $K \leqslant Q_R$

$$\rho_R(\lambda_Q(I)) = I \quad \text{и} \quad \lambda_Q(\rho_R(K)) = K.$$

Для каждого коммутативного артинова кольца существует единственный (с точностью до изоморфизма) QF-модуль Q_R [8, 11], причём $(Q, +) \cong (R, +)$. Кольцо R называется *квазифробениусовым* (*QF-кольцом*), если R_R — QF-модуль.

Квазифробениусовы кольца и модули играют ключевую роль в теории кодов и рекуррентных последовательностей.

Теорема 1.4. *Для всякого коммутативного кольца R эквивалентны следующие условия*:

1) *R — квазифробениусово кольцо, допускающее мультипликативный порядок на одночленах*;
2) *R — локальное артиново кольцо главных идеалов.*

Доказательство. Докажем импликацию 1) $\Longrightarrow$ 2). Согласно предложению 1.3 для любых $a, b \in R$ или $\mathrm{An}(aR) \subseteq \mathrm{An}(bR)$, или $\mathrm{An}(bR) \subseteq \mathrm{An}(aR)$. Кольцо R квазифробениусово, так что $aR = \mathrm{An}(\mathrm{An}(aR))$ и $bR = \mathrm{An}(\mathrm{An}(bR))$. Значит, или $aR \subseteq bR$, или $bR \subseteq aR$, то есть главные идеалы из R образуют цепь.

Кольцо R артиново, а значит, нётерово, и, следовательно, всякий его идеал $I \lhd R$ конечно порождён:

$$I = a_1R + \ldots + a_mR.$$

Ясно, что $I = a_sR$, где a_sR — наибольший из главных идеалов $a_1R, \ldots, a_mR$. Таким образом, R является артиновым цепным кольцом главных идеалов, откуда легко следует 2).

Проверим импликацию 2) $\Longrightarrow$ 1). Пусть R — локальное артиново кольцо главных идеалов. Проверим, что для R выполняются условия из пункта 2) предложения 1.3.

Структура идеалов кольца R такова:

$$R > \pi R > \pi^2 R > \ldots > \pi^{n-1}R > \pi^n R = 0, \tag{1.6}$$

где n — индекс нильпотентности радикала Джекобсона $J = \mathrm{rad}(R)$ и π — либо произвольный элемент из $J \setminus J^2$ (при $n > 1$), либо 0 (при $n = 1$). Значит, R — цепное кольцо и, следовательно, предпорядок $\lesssim_{\mathrm{An}}$ линеен. Справедливость условия (1.4) следует из (1.6) и того, что для любого $a = \alpha\pi^i$, $\alpha \in R^*$, $i \in \overline{0,n}$,

$$\mathrm{An}(a) = \pi^{n-i}R. \quad \square$$

Следует отметить, что, как показывают приводимые ниже примеры, существуют кольца, допускающие мультипликативный порядок на одночленах и не удовлетворяющие условиям предыдущей теоремы.

Пример 1.5. Всякое коммутативное локальное кольцо R, для которого $[\mathrm{rad}(R)]^2 = 0$, допускает мультипликативный порядок на одночленах. Действительно, если $J = \mathrm{rad}(R) = 0$, то R — поле, и наше утверждение очевидно. Пусть $J \neq 0$, тогда для любого $a \in R$

$$\mathrm{An}(a) = \begin{cases} R & \text{при } a = 0, \\ J & \text{при } a \in J \setminus 0, \\ 0 & \text{при } a \in R^* = R \setminus J, \end{cases}$$

откуда следует, что для R выполняются условия из пункта 2) предложения 1.3.

Пример 1.6. Пусть P — поле, $P[x_1, \ldots, x_k]$ — кольцо полиномов и $I = (x_1, \ldots, x_k)^m$. Положим $R = P[X]/I$. Очевидно, что R — локальное артиново кольцо и $J = \mathrm{rad}(R) = (\theta_1, \ldots, \theta_k)$, где $\theta_i = x_i + I$, $i \in \overline{1,k}$. Всякий элемент $a \in R$ однозначно представляется в виде

$$a = \sum_{\substack{i_1,\ldots,i_k \in \mathbb{N}_0, \\ i_1+\ldots+i_k<m}} \alpha_{i_1\ldots i_k}\theta_1^{i_1}\ldots\theta_k^{i_k}, \tag{1.7}$$

где $\alpha_{i_1\ldots i_k} \in P$. Для каждого элемента $a \neq 0$ определим параметр

$$s(a) = \min\{i_1 + \ldots + i_k \mid \alpha_{i_1\ldots i_k} \neq 0\}.$$

Таким образом, $s(a)$ — это наименьшая из степеней мономов, входящих в представление (1.7) элемента a. Положим также $s(0) = m$.

Легко проверить, что для любых $a, b \in R$

$$s(ab) = \min\{s(a) + s(b), m\}. \tag{1.8}$$

Из соотношения (1.8) следует, что для $a \in R$

$$\mathrm{An}(a) = J^{m-s(a)}$$

(здесь мы полагаем, что $J^0 = R$) и, следовательно,

$$a \lesssim_{\mathrm{An}} b \iff s(a) \geqslant s(b).$$

Отсюда и из (1.8) следует, что для R выполняются условия из пункта 2) предложения 1.3.

Всюду далее мы полагаем, что R — коммутативное артиново локальное кольцо главных идеалов со структурой идеалов (1.6).

При заданном линейном порядке $\preceq$ на $[X]$ формула

$$au \prec bv \overset{\text{def}}{\Longleftrightarrow} u \prec v \text{ и } a, b \neq 0$$

определяет разделяющий мономы порядок на $[R, X]$. Именно такое упорядочение одночленов использовались в большинстве предыдущих работ при определении ведущего члена полинома, редукций на полиномах и стандартных базисов идеалов (см. [12, 14, 15, 23]). Как следует из предложения 1.1, этот порядок при $n > 1$ не является мультипликативным. Вместе с тем из теоремы 1.4 следует, что мультипликативный порядок на $[R, X]$ существует. Один из таких порядков рассматривался в [7], а затем и в [9,10], что привело к построению стандартного базиса (названного авторами *канонической системой образующих* (КСО)), более эффективного при решении ряда прикладных задач (см. [7, 9, 10]).

Основная цель этого раздела — определение и изучение порядков $\preceq$ и $\preceq^{\Gamma}$ на $R[X]$, которые будут использованы в дальнейшем при построении кольцевых схем симплификации $\mathfrak{G}$ и $\mathfrak{G}^{\Gamma}$.

Определим, как и в [7], *нормы* элемента $r \in R$, полинома $F \in R[X]$ и подмножества $\chi \subset R[X]$ равенствами

$$\begin{aligned} \|r\| &= \max\{i \in \overline{0,n} \mid r \in \pi^i R\}, \\ \|F\| &= \max\{i \in \overline{0,n} \mid F \in \pi^i R[X]\}, \\ \|\chi\| &= \max\{i \in \overline{0,n} \mid \chi \subseteq \pi^i R[X]\}. \end{aligned} \tag{1.9}$$

Нормы (1.9) обладают следующими свойствами:

$$\begin{aligned} \|ab\| &= \min(\|a\| + \|b\|, n), \\ \|a + b\| &\geqslant \min(\|a\|, \|b\|) \end{aligned} \tag{1.10}$$

для любых $a, b \in R$. Аналогичные соотношения верны для полиномов из $R[X]$.

Мультипликативный порядок на $[R, X]$ может не удовлетворять условию обрыва убывающих цепочек, однако для сходимости многих описываемых ниже алгоритмов это условие критично. Ввиду этого порядок на $[R, X]$ мы будем строить как продолжение (см. предложение 1.3) некоторого полного порядка на $[X]$.

Предложение 1.7 (см., например, [5]). *Линейно упорядоченная полугруппа* $([X], \cdot, \preceq)$ *является вполне упорядоченной полугруппой, если и только если* $1 \preceq u$ *для любого* $u \in [X]$. *В этом случае порядок* $\preceq$ *называется* допустимым.

Определение 1.8. *Полугруппой* π*-мономов* назовём подполугруппу

$$[\pi, X] = [\pi, x_1, \ldots, x_k] = \{\pi^a u \mid a \in \overline{0, n-1};\ u \in [X]\} \cup \{0\}$$

полугруппы $(R[X], \cdot)$. Формально:

$$[\pi, X] = \langle x_0, x_1, \ldots, x_k \mid x_i x_j = x_j x_i,\ x_0^n x_l = x_0^n;\ i, j, l \in \overline{0,k} \rangle.$$

Очевидно, что полугруппа $[X]$ является подполугруппой полугруппы $[\pi, X]$. Пусть на $[X]$ задан некоторый допустимый порядок $\preceq$. Тогда на $[\pi, X]$ можно ввести два порядка $\preceq_-$ и $\preceq_+$.

Определим $\preceq_-$:

$$\begin{aligned} &\pi^a u \preceq_- \pi^b v \overset{\text{def}}{\iff} \begin{cases} a > b \ \text{ или} \\ a = b \text{ и } u \preceq v, \end{cases} \\ &\forall U \in [\pi, X]\ 0 \preceq_- U, \end{aligned} \tag{1.11}$$

где $a, b \in \overline{0, n-1}$, $u, v \in [X]$.

Симметрично определяется порядок $\preceq_+$:

$$\begin{aligned} &\pi^a u \preceq_+ \pi^b v \overset{\text{def}}{\iff} \begin{cases} a < b \ \text{ или} \\ a = b \text{ и } u \preceq v, \end{cases} \\ &\forall U \in [\pi, X]\ U \preceq_+ 0, \end{aligned} \tag{1.12}$$

где $a, b \in \overline{0, n-1}$, $u, v \in [X]$.

Легко видеть, что каждый из порядков $\preceq_-$ и $\preceq_+$ превращает $[\pi, X]$ во вполне упорядоченную полугруппу, в которой $([X], \cdot, \preceq)$ — упорядоченная подполугруппа. Более того, как показывает следующее утверждение, других порядков с таким свойством нет.

Предложение 1.9 ([2, предложение 3]). *Пусть на $[\pi, X]$ задан такой порядок $\leqslant$, что $([\pi, X], \cdot, \leqslant)$ — вполне упорядоченная полугруппа и $\preceq$ — ограничение $\leqslant$ на $[X]$. Тогда $\leqslant$ совпадает с $\preceq_-$ или $\preceq_+$.*

Всякий линейный порядок $\preceq$ на $[\pi, X]$ следующим образом продолжается до разделяющего мономы порядка $\preceq$ на $[R, X]$: для любых $U, V \in [\pi, X]$ и $a, b \in R^*$

$$aU \prec bV \overset{\text{def}}{\iff} U \prec V. \tag{1.13}$$

С учётом предложений 1.1 и 1.9 легко доказать следующее утверждение.

Предложение 1.10. *Пусть $\pi \neq 0$ и $\preceq$ — такой порядок на $[\pi, X]$, что $([\pi, X], \cdot, \preceq)$ — вполне упорядоченная полугруппа. Тогда эквивалентны следующие условия*:

1) *упорядочение на $[R, X]$, определяемое соотношением* (1.13)*, является мультипликативным*;
2) $(U \preceq V,\ VW = 0) \implies (UW = 0)$ *для любых $U, V, W \in [\pi, X]$.*

Ввиду предложения 1.10 мы принимаем следующее определение.

Определение 1.11. *Допустимым порядком* на $[\pi, X]$ будем называть такой порядок $\preceq$, что

1) $([\pi, X], \cdot, \preceq)$ — вполне упорядоченная полугруппа;
2) $(U \preceq V,\ VW = 0) \implies (UW = 0)$ для любых $U, V, W \in [\pi, X]$.

Для допустимого порядка $\preceq$ на $[X]$ продолжение $\preceq_-$ на $[\pi, X]$ является допустимым порядком, а продолжение $\preceq_+$ — нет. Ввиду этого *естественным продолжением* порядка $\preceq$ на $[\pi, X]$ будем называть порядок $\preceq_-$ и, поскольку в дальнейшем порядок $\preceq_+$ использоваться не будет, для обозначения рассматриваемого продолжения будем употреблять прежний символ $\preceq$.

Легко проверяется следующее утверждение.

Предложение 1.12. *Всякий допустимый порядок $\preceq$ на $[\pi, X]$ обладает следующими свойствами:*

$$U \preceq V \implies \|U\| \geqslant \|V\|, \tag{1.14}$$

$$\|U\| > \|V\| \implies U \prec V, \tag{1.15}$$

$$U \prec V,\ VW \neq 0 \implies UW \prec VW \tag{1.16}$$

для любых π-мономов $U, V, W \in [\pi, X]$.

Пусть $F \in R[X]$ и $u \in [X]$. Элемент из R, являющийся коэффициентом при мономе u в полиноме F, обозначим через $\mathrm{Cf}(F, u)$.

Носителем многочлена $F \in R[x]$ называется множество

$$\mathrm{supp}(F) = \{u \in [X] \mid \mathrm{Cf}(F, u) \neq 0\}. \tag{1.17}$$

Назовём *π-носителем* многочлена $F \in R[x]$ множество

$$\mathrm{Supp}(F) = \{U \in [\pi, X] \mid U = \pi^{\|\mathrm{Cf}(F,u)\|}u,\ u \in \mathrm{supp}(F)\}. \tag{1.18}$$

Пусть на $[\pi, X]$ задан некоторый допустимый порядок $\preceq$. Пусть также дан некоторый полином $F \in R[X] \setminus 0$. Тогда π-носитель $\mathrm{Supp}(F)$ непуст и в нём существует наибольший относительно порядка $\preceq$ π-моном $V_0 = \pi^{a_0}v_0 \in [\pi, X]$. В этой ситуации мы будем использовать следующую терминологию:

$$\mathrm{Lm}(F) = v_0 \text{ — } \textit{ведущий моном } F,$$
$$\mathrm{Lc}(F) = \mathrm{Cf}(F, v_0) \text{ — } \textit{ведущий коэффициент } F,$$
$$\mathrm{Lt}(F) = \mathrm{Lc}(F)\,\mathrm{Lm}(F) \text{ — } \textit{ведущий член } F,$$
$$\mathrm{LM}(F) = \pi^{\|\mathrm{Lc}(F)\|}\,\mathrm{Lm}(F) = V_0 \text{ — } \textit{ведущий } \pi\textit{-моном } F.$$

Положим также по определению $\mathrm{Lc}(0) = \mathrm{Lt}(0) = \mathrm{LM}(0) = 0$ (значение $\mathrm{Lm}(0)$ считаем неопределённым). Ясно, что функция Lt совпадает с $\mathrm{lt}_\preceq$ для мультипликативного порядка $\preceq$ на $[R, X]$, получающегося продолжением рассматриваемого допустимого порядка по формуле (1.13).

Для произвольного подмножества $\chi \subseteq R[X]$ обозначим через $\mathrm{Lm}(\chi)$ множество всех различных ведущих мономов полиномов из χ: $\mathrm{Lm}(\chi) = \{\mathrm{Lm}(G) \mid G \in \chi\}$. Аналогичные обозначения используем и для остальных введённых выше функций Lc, Lt, LM.

Замечание 1.13. Для любого полинома F верны равенства $\|F\| = \|\mathrm{Lc}(F)\| = \|\mathrm{Lt}(F)\| = \|\mathrm{LM}(F)\|$.

Из определения 1.11 и предложений 1.10, 1.12 легко вытекает следующее утверждение.

Предложение 1.14. *Для любых полиномов $F, G \in R[X]$ выполняются соотношения*

$$\operatorname{Lm}(FG) = \operatorname{Lm}(F)\operatorname{Lm}(G) \quad \textit{при} \quad FG \neq 0,$$
$$\operatorname{LM}(FG) = \operatorname{LM}(F)\operatorname{LM}(G).$$

Если к тому же F или G является одночленом, то

$$\operatorname{Lc}(FG) = \operatorname{Lc}(F)\operatorname{Lc}(G),$$
$$\operatorname{Lt}(FG) = \operatorname{Lt}(F)\operatorname{Lt}(G).$$

Как показывает следующий пример, во второй паре равенств из предложения 1.14 в общем случае нельзя обойтись без сформулированных дополнительных условий на F и G, так как за счёт приведения подобных членов значение ведущего коэффициента может измениться.

Пример 1.15. Рассмотрим кольцо полиномов $\mathbb{Z}_8[x_1, x_2]$. Положим $\pi = 2$ и зафиксируем некоторый допустимый порядок на $[2, x_1, x_2]$. Полиномы $F = x_1 + 2x_2$ и $G = x_2 + 2x_1$ таковы, что $\operatorname{Lc}(FG) = \operatorname{Lc}(5x_1x_2 + 2x_1^2 + 2x_2^2) = 5 \neq 1 \cdot 1 = \operatorname{Lc}(F)\operatorname{Lc}(G)$.

Предложение 1.16. *Пусть Γ — семейство представителей классов вычетов R по πR. Тогда для любого $a \in R$ существует единственный вектор $(a_0, a_1, \ldots, a_{n-1}) \in \Gamma^n$, такой что*

$$a = a_0 + \pi a_1 + \ldots + \pi^{n-1} a_{n-1}. \tag{1.19}$$

Доказательство. Существование указанного вектора очевидно, проверим единственность. Пусть $a = b_0 + \pi b_1 + \ldots + \pi^{n-1} b_{n-1}$, где $b_i \in \Gamma$, $i \in \overline{0, n-1}$. Очевидно, что $b_0 = a_0$. Пусть уже доказано, что $b_0 = a_0, \ldots, b_i = a_i$, $i \in \overline{0, n-2}$, тогда $\pi^{i+1} b_{i+1} + \ldots + \pi^{n-1} b_{n-1} = \pi^{i+1} a_{i+1} + \ldots + \pi^{n-1} a_{n-1}$. Отсюда следует, что $b_{i+1} - a_{i+1} \in \pi R$, и, значит, $b_{i+1} = a_{i+1}$. □

В условиях предложения 1.16 мы пишем $a_i = \gamma_i^\Gamma(a)$, $i \in \overline{0, n-1}$. Если из контекста ясно, какое семейство представителей классов вычетов рассматривается, мы пишем $\gamma_i(a)$ вместо $\gamma_i^\Gamma(a)$.

Зафиксируем некоторое семейство представителей классов вычетов $\Gamma \subseteq R$ $(0 \in \Gamma)$ для $R/\pi R$. *Координатным π-носителем* многочлена $F \in R[X]$ назовём множество

$$\operatorname{Supp}^\Gamma(F) = \{\pi^i u \mid u \in \operatorname{supp}(F),\ i \in \overline{0, n-1},\ \gamma_i(\operatorname{Cf}(F, u)) \neq 0\}. \tag{1.20}$$

Пусть M — некоторое непустое множество и M_{fin} — множество всех конечных подмножеств M:

$$M_{\text{fin}} = \{X \subseteq M \mid |X| < \aleph_0\}. \tag{1.21}$$

Предположим, что на M задан некоторый линейный порядок $\preceq$. Он индуцирует линейный порядок $\preceq$ на M_{fin}. А именно, пусть $A = \{a_1, \ldots, a_m\}$ и $B = \{b_1, \ldots, b_n\}$ — непустые множества из M_{fin}, причём $a_1 \succ \ldots \succ a_m$ и

$b_1 \succ \ldots \succ b_n$, положим

$$A \preceq B \overset{\text{def}}{\Longleftrightarrow} \begin{cases} m \leqslant n \text{ и } a_i = b_i,\ i \in \overline{1,m}, & \text{или} \\ \exists k \leqslant \min\{m,n\}\ a_1 = b_1, \ldots, a_{k-1} = b_{k-1},\ a_k \prec b_k. \end{cases} \tag{1.22}$$

Также для любого $C \in M_{\text{fin}}$ по определению полагаем $\varnothing \preceq C$. Иными словами, построенный на M_{fin} порядок $\preceq$ сводится к лексикографическому сравнению слов, получающихся из множеств выписыванием их элементов по убыванию.

Предложение 1.17 (см., например, [2]). *Упорядоченное множество $(M_{\text{fin}}, \preceq)$ является вполне упорядоченным тогда и только тогда, когда $(M, \preceq)$ — вполне упорядоченное множество.*

Пусть на $[X]$ задан некоторый допустимый порядок $\preceq$. Его естественное продолжение на $[\pi, X]$ индуцирует порядок $\preceq$ на $[\pi, X]_{\text{fin}}$. Для любого полинома $F \in R[X]$ носители $\operatorname{Supp}(F)$ и $\operatorname{Supp}^{\Gamma}(F)$ являются элементами $[\pi, X]_{\text{fin}}$, и мы по определению полагаем

$$\begin{aligned} F \prec G &\overset{\text{def}}{\Longleftrightarrow} \operatorname{Supp}(F) \prec \operatorname{Supp}(G), \\ F \prec^{\Gamma} G &\overset{\text{def}}{\Longleftrightarrow} \operatorname{Supp}^{\Gamma}(F) \prec \operatorname{Supp}^{\Gamma}(G). \end{aligned} \tag{1.23}$$

При этом $F \preceq G \overset{\text{def}}{\Longleftrightarrow} (F \prec G) \vee (F = G)$ и аналогично для $\preceq^{\Gamma}$.

Замечание 1.18. Отметим, что построенные порядки $\preceq$ и $\preceq^{\Gamma}$ в общем случае не будут линейными. Например, в кольце $\mathbb{Z}_9[x]$ полиномы x и $2x$ несравнимы (при единственном допустимом порядке $\preceq$ на $[x]$ и $\Gamma = \{0,1,2\}$).

В качестве непосредственного следствия предложения 1.17 получаем следующее утверждение.

Предложение 1.19. *Пусть заданы допустимый порядок $\preceq$ на $[X]$ и семейство представителей классов вычетов $\Gamma \subseteq R$. Тогда отношения $\preceq$ и $\preceq^{\Gamma}$, определяемые формулой* (1.23)*, являются отношениями частичного порядка на $R[X]$, удовлетворяющими условию минимальности.*

Итак, двигаясь по цепочке

$$[X],\ [\pi, X],\ [\pi, X]_{\text{fin}},\ R[X],$$

мы продолжили допустимый порядок $\preceq$ на $[X]$ до порядков $\preceq$ и $\preceq^{\Gamma}$ на $R[X]$. Отметим также, что упорядочение одночленов, получаемое ограничением порядка $\preceq$ на $[R, X]$, рассматривалось ранее в [7, 9, 10].

В дальнейшем, когда задан некоторый допустимый порядок на $[X]$, порядки на $[\pi, X]$, $[\pi, X]_{\text{fin}}$ и $R[X]$ также предполагаются заданными.

1.2. Схемы симплификации

При построении стандартного базиса полиномиального идеала мы существенно используем язык схем симплификации из [6].

Определение 1.20. Пусть $(M, \preceq)$ — непустое упорядоченное множество с условием минимальности и $S \subseteq M^M$. Тройка $\mathfrak{S} = (M, \preceq, S)$ называется *схемой симплификации* на M, если выполнено условие

$$\forall m \in M \ \forall s \in S \ s(m) \preceq m. \tag{1.24}$$

При этом порядок $\preceq$ называется *порядком сложности*. Элементы из S называются (*одношаговыми*) *симплификаторами* или (*элементарными*) *редукциями*.

Определение 1.21. Пусть $\mathfrak{S} = (M, \preceq, S)$ — схема симплификации. Говорят, что $m \in M$ — *нормальный*, или *редуцированный*, элемент (относительно $\mathfrak{S}$), если $s(m) = m$ для любого $s \in S$, в противном случае элемент m называют *редуцируемым*. Совокупность всех нормальных элементов обозначается $N_{\mathfrak{S}}$.

Отметим, что $N_{\mathfrak{S}} \neq \varnothing$, поскольку $\preceq$ удовлетворяет условию минимальности и $N_{\mathfrak{S}}$ содержит все минимальные элементы множества M.

Обозначим через $\hat{S}$ подполугруппу в полугруппе M^M (с композицией функций в качестве умножения), порождённую $S \cup \{1_M\}$, то есть

$$\hat{S} = |S, 1_M\rangle = \{s_1 \circ \ldots \circ s_n \mid (n \in \mathbb{N}) \wedge (\forall i \in \overline{1,n} \ s_i \in S)\} \cup \{1_M\}. \tag{1.25}$$

Элементы из $\hat{S}$ назовём *редукциями* или *симплификаторами* (неодношаговыми).

Определение 1.22. Пусть $\mathfrak{S} = (M, \preceq, S)$ — схема симплификации. *Множество нормальных форм* элемента $m \in M$ определяется равенством

$$\mathrm{Nor}_{\mathfrak{S}}(m) = \hat{S}(m) \cap N_{\mathfrak{S}}. \tag{1.26}$$

Любой элемент из $\mathrm{Nor}_{\mathfrak{S}}(m)$ называется *нормальной формой* m. Так как порядок $\preceq$ удовлетворяет условию минимальности, множество нормальных форм любого элемента $m \in M$ непусто. Для произвольного подмножества $L \subseteq M$ мы также определяем

$$\mathrm{Nor}_{\mathfrak{S}}(L) = \bigcup_{l \in L} \mathrm{Nor}_{\mathfrak{S}}(l). \tag{1.27}$$

Например, $\mathrm{Nor}_{\mathfrak{S}}(M) = N_{\mathfrak{S}}$ — множество всех нормальных элементов.

Определение 1.23. Пусть $\mathfrak{S} = (M, \preceq, S)$ — схема симплификации. Если $|\mathrm{Nor}_{\mathfrak{S}}(m)| = 1$, то говорят, что $m \in M$ обладает *канонической формой*. В этом случае элемент $\mathrm{Can}_{\mathfrak{S}}(m) \in M$, определяемый из равенства $\mathrm{Nor}_{\mathfrak{S}}(m) = \{\mathrm{Can}_{\mathfrak{S}}(m)\}$, называется *канонической формой* m.

Множество всех элементов из M, обладающих канонической формой, обозначается $C_{\mathfrak{S}}$.

Если $C_{\mathfrak{S}} = M$, то говорят, что $\mathfrak{S}$ — схема симплификации с *канонизацией*.

Очевидно, что $N_{\mathfrak{S}} \subseteq C_{\mathfrak{S}}$ и $\mathrm{Can}_{\mathfrak{S}}(C_{\mathfrak{S}}) = N_{\mathfrak{S}}$. Поэтому мы можем рассматривать $\mathrm{Can}_{\mathfrak{S}}$ как отображение из $C_{\mathfrak{S}}$ в $C_{\mathfrak{S}}$.

Для краткости, когда из контекста ясно, какая схема симплификации рассматривается, мы будем писать N, Nor, Can и C вместо $N_{\mathfrak{S}}$, $\mathrm{Nor}_{\mathfrak{S}}$, $\mathrm{Can}_{\mathfrak{S}}$ и $C_{\mathfrak{S}}$ соответственно.

Лемма 1.24 (см., например, [2]). *Пусть $\mathfrak{S} = (M, \preceq, S)$ — схема симплификации. Тогда для любых элементов $m_1, \ldots, m_t$ из M существует симплификатор $\sigma \in \hat{S}$, такой что $\sigma(m_i) \in \mathrm{Nor}(m_i)$ для всех $i \in \overline{1,t}$.*

Определение 1.25. Пусть R — кольцо и M_R — правый R-модуль. Схема симплификации $\mathfrak{S} = (M_R, \preceq, S)$ называется *R-линейной*, если $S \subseteq \mathrm{End}(M_R)$.

Предложение 1.26 (см., например, [2]). *Пусть $\mathfrak{S} = (M_R, \preceq, S)$ — R-линейная схема симплификации. Тогда $C = C_{\mathfrak{S}}$ и $N = N_{\mathfrak{S}}$ — подмодули в M_R. Отображение $\mathrm{Can}\colon C \to C$ является проектором, то есть $\mathrm{Can} \in \mathrm{End}(C_R)$ и $\mathrm{Can}^2 = \mathrm{Can}$ (и, стало быть, $C = \mathrm{Im}(\mathrm{Can}) \oplus \mathrm{Ker}(\mathrm{Can}) = N \oplus \mathrm{Ker}(\mathrm{Can})$).*

В заключение этого раздела мы рассмотрим общее определение стандартного базиса, которое понадобится нам в дальнейшем.

Определение 1.27. Пусть R — кольцо и $M = M_R$ — правый модуль. Схему симплификации $\mathfrak{S} = (M, \preceq, S)$ на M_R будем называть *консервативной*, если определено *отображение сечения*[1]

$$\delta\colon P(M) \to P(S),$$
$$\delta\colon M \supseteq \chi \mapsto S_\chi \subseteq S,$$

такое что для любых элемента $x \in M$ и симплификатора $s \in S_\chi$

$$x - sx \in \chi R.$$

Аналогично определяем консервативные схемы симплификации на левых модулях и на бимодулях.

Сечением консервативной схемы симплификации $\mathfrak{S} = (M, \preceq, S)$ *относительно* $\chi \subseteq M$ назовём схему симплификации $\mathfrak{S}_\chi = (M, \preceq, S_\chi)$. Ясно, что сечение $\mathfrak{S}_\chi$ является консервативной схемой симплификации с отображением сечения

$$\delta_\chi\colon P(M) \to P(S_\chi), \quad \delta_\chi(\psi) = \delta(\psi) \cap S_\chi.$$

Предложение 1.28. *Пусть $\mathfrak{S}$ — консервативная схема симплификации на M_R, A — подмодуль в M_R и $\chi \subseteq A$, тогда эквивалентны следующие условия*:

1) $\mathrm{Nor}_{\mathfrak{S}_\chi}(a) \ni 0$ *для любого* $a \in A$;
2) $\mathrm{Nor}_{\mathfrak{S}_\chi}(a) = 0$ *для любого* $a \in A$.

Доказательство. Докажем импликацию 1) $\Longrightarrow$ 2). Пусть $a \in A$ и $x \in \mathrm{Nor}_{\mathfrak{S}_\chi}(a)$. Тогда согласно определению консервативной схемы симплификации $x - a \in \chi R$ и, значит, $x \in A$. Элемент x нормален относительно $\mathfrak{S}_\chi$, и, следовательно, $\mathrm{Nor}_{\mathfrak{S}_\chi}(x) = \{x\}$. Наконец, 1) влечёт $x = 0$.

Импликация 2) $\Longrightarrow$ 1) очевидна. □

Определение 1.29. В условиях предложения 1.28 множество χ, удовлетворяющее эквивалентным условиям 1), 2), назовём *$\mathfrak{S}$-стандартным базисом* подмодуля A. Множество $\chi \subseteq M$ будем называть *$\mathfrak{S}$-стандартной системой*, если χ — *$\mathfrak{S}$-стандартный базис* для $\chi R \leqslant M_R$.

[1] Здесь $P(M) = \{X \mid X \subseteq M\}$ — множество всех подмножеств M.

Очевидно, что если χ является $\mathfrak{S}$-стандартным базисом подмодуля $A \leqslant M_R$, то $A = \chi R$.

Определению 1.29 удовлетворяют все известные автору стандартные базисы подмодулей модуля $R[x_1, \ldots, x_k]^d$, в частности (при $d = 1$) стандартные базисы полиномиальных идеалов (см. [5, 7, 9, 10, 12, 14, 15, 23]).

Скажем, что консервативная схема симплификации $\mathfrak{T} = (M, \preceq', T)$ *подчинена* $\mathfrak{S}$, если всякая $\mathfrak{T}$-стандартная система является $\mathfrak{S}$-стандартной системой. Очевидно, что $\mathfrak{T}$ подчинена $\mathfrak{S}$ тогда и только тогда, когда всякий $\mathfrak{T}$-стандартный базис произвольного подмодуля $A \leqslant M_R$ будет $\mathfrak{S}$-стандартным базисом A.

Схемы симплификации $\mathfrak{T}$ и $\mathfrak{S}$ назовём *эквивалентными*, если $\mathfrak{T}$ подчинена $\mathfrak{S}$ и $\mathfrak{S}$ подчинена $\mathfrak{T}$.

Предложение 1.30. *Пусть $\mathfrak{S} = (M, \preceq, S)$ и $\mathfrak{T} = (M, \preceq', T)$ — консервативные схемы симплификации на M_R. Тогда если*

$$\forall \chi \subseteq M \ \forall x \in M \ \operatorname{Nor}_{\mathfrak{T}_\chi}(x) \ni 0 \implies \operatorname{Nor}_{\mathfrak{S}_\chi}(x) \ni 0, \tag{1.28}$$

то схема симплификации $\mathfrak{T}$ подчинена $\mathfrak{S}$.

Если к тому же 0 — нормальный элемент относительно $\mathfrak{S}$ и $\mathfrak{T}$, то условие (1.28) *равносильно*

$$\forall \chi \subseteq M \ \forall x \in M \ \hat{T}_\chi x \ni 0 \implies \hat{S}_\chi x \ni 0. \tag{1.29}$$

Доказательство. Первая часть предложения очевидна. Вторая часть следует из того, что если $0 \in N_{\mathfrak{S}}$, то $0 \in N_{\mathfrak{S}_\chi}$ для любого $\chi \subseteq M$ и, значит,

$$\operatorname{Nor}_{\mathfrak{S}_\chi}(x) \ni 0 \iff \hat{S}_\chi x \ni 0. \quad \square$$

Из предложения 1.28 следует, что предложение 1.30 остаётся справедливым, если в условии (1.28) каждый символ «$\ni$» заменить на «$=$».

Следствие 1.31. *Пусть $\mathfrak{S} = (M, \preceq, S)$ и $\mathfrak{T} = (M, \preceq', T)$ — консервативные схемы симплификации на M_R, такие что $0 \in N_{\mathfrak{S}}$ и $0 \in N_{\mathfrak{T}}$. Тогда если*

$$\forall \chi \subseteq M \ \forall x \in M \ T_\chi x \subseteq \hat{S}_\chi x,$$

то схема симплификации $\mathfrak{T}$ подчинена $\mathfrak{S}$.

1.3. Схемы симплификации на полиномах

Мы построим консервативные схемы симплификации $\mathfrak{G} = (R[X], \preceq, S)$ и $\mathfrak{G}^\Gamma = (R[X], \preceq^\Gamma, S^\Gamma)$ на $R[X]$. Основным множеством для обеих схем симплификации является алгебра полиномов $R[X] = R[x_1, \ldots, x_k]$ от k коммутирующих переменных над кольцом R. Порядки сложности $\preceq$ и $\preceq^\Gamma$ были определены в разделе 1.1. Построим последние элементы наших схем симплификации — семейства редукций S и S^Γ.

Зафиксируем некоторый допустимый порядок $\preceq$ на полугруппе мономов $[X]$ и семейство представителей классов вычетов $\Gamma \subseteq R$ $(0 \in \Gamma)$ для $R/\pi R$.

Пусть даны полином $G \in R[X] \setminus 0$ с ведущим коэффициентом $a = \mathrm{Lc}(G)$ и моном $u \in [X]$. Определим редукцию $r_{G,u}\colon R[X] \to R[X]$. Для любого $F \in R[X]$ если $c = \mathrm{Cf}(F, u\,\mathrm{Lm}(G))$, то

$$r_{G,u}(F) = \begin{cases} F, & \text{если } \|c\| < \|a\|, \\ F - buG, & \text{если } \|c\| \geqslant \|a\|,\ c = ba. \end{cases} \tag{1.30}$$

Отметим, что данное определение не зависит от выбора элемента b. Действительно, для другого элемента $b' \in R$, такого что $c = b'a$, будем иметь $(b - b')\,\mathrm{Lc}(G) = (b - b')a = 0 \implies (b - b')G = 0 \implies F - buG = F - b'uG$.

Для любого монома $u \in [X]$ полагаем $r_{0,u} = 1_{R[X]}$.

Заметим, что $r_{G,u}(F) = F$, в точности если $\|c\| < \|a\|$ или $c = 0$ (в последнем случае $buG = 0$).

Определение 1.32. Полином $F \in R[X] \setminus 0$ назовём *π-унитарным*, если

$$\mathrm{Lc}(F) = \pi^{\|F\|}.$$

Для любого полинома $F \in R[X]$ существуют элемент $a \in R^*$ и такой π-унитарный полином $\mathring{F}$, что $F = a\mathring{F}$. Как показано в [2], полином $\mathring{F}$ определяется по F однозначно.

Пусть даны полином $F \in R[X]$ и π-моном $V = \pi^i v \in [\pi, X] \setminus 0$. Нам будет удобно пользоваться следующим обозначением:

$$\mathrm{Cf}^\Gamma(F, V) = \gamma_i^\Gamma(\mathrm{Cf}(F, v)).$$

Также для любого $F \in R[X]$ полагаем $\mathrm{Cf}^\Gamma(F, 0) = 0$. Ясно, что $\mathrm{Supp}^\Gamma(F) = \{V \in [\pi, X] \mid \mathrm{Cf}^\Gamma(F, V) \neq 0\}$ и

$$F = \sum_{V \in \mathrm{Supp}^\Gamma(F)} \mathrm{Cf}^\Gamma(F, V)V.$$

Пусть даны полином $G \in R[X]$ и π-моном $U \in [\pi, X]$. Определим редукцию $r^\Gamma_{G,\,U}\colon R[X] \to R[X]$. Для любого $F \in R[X]$

$$r^\Gamma_{G,\,U}(F) = F - \mathrm{Cf}^\Gamma(F, U\,\mathrm{LM}(G)) \cdot U\mathring{G}. \tag{1.31}$$

Очевидно, что $r^\Gamma_{G,U}(F) = F$, в точности если $\mathrm{Cf}^\Gamma(F, U\,\mathrm{LM}(G)) = 0$.

Следует отметить, что используемая в (1.31) идея построения редукций, апеллирующих к разложению (1.19), была реализована ранее в [14] для колец Галуа (при другом понятии ведущего члена полинома).

Предложение 1.33. *Пусть даны полином $G \in R[X]$, моном $u \in [X]$ и π-моном $U \in [\pi, X]$. Тогда для любого полинома $F \in R[X]$*

1) $r_{G,u}(F) \preceq F$ *и* $r^\Gamma_{G,U}(F) \preceq^\Gamma F$;
2) $\|F\| \leqslant \|r_{G,u}(F)\|$ *и* $\|F\| \leqslant \|r^\Gamma_{G,U}(F)\|$.

Доказательство. Первое неравенство из пункта 1) было доказано в [2, предложение 7]. Докажем второе неравенство.

Если $c = \mathrm{Cf}^\Gamma(F, U\,\mathrm{LM}(G)) = 0$, то $r_{G,u}(F) = F$ и наше утверждение верно. Остаётся рассмотреть ситуацию, когда $c \neq 0$.

Пусть $c_V = \mathrm{Cf}^\Gamma(F, V)$ и $d_V = \mathrm{Cf}^\Gamma(G, V)$, $V \in [\pi, X]$. Мы имеем

$$F = \sum_{V \succ U\,\mathrm{LM}(G)} c_V V + cU\,\mathrm{LM}(G) + \sum_{V \prec U\,\mathrm{LM}(G)} c_V V$$

и

$$cU\mathring{G} = cU\,\mathrm{LM}(G) + \sum_{V \prec U\,\mathrm{LM}(G)} d_V V.$$

Значит,

$$r^\Gamma_{G,u}(F) = \sum_{V \succ U\,\mathrm{LM}(G)} c_V V + \sum_{V \prec U\,\mathrm{LM}(G)} (c_V - d_V)V. \tag{1.32}$$

В силу (1.10) все элементы координатного π-носителя второй суммы из (1.32) младше $U\,\mathrm{LM}(G)$. Тогда $\mathrm{Supp}^\Gamma(r^\Gamma_{G,U}(F)) \prec \mathrm{Supp}^\Gamma(F)$ и, значит, $r^\Gamma_{G,U}(F) \prec^\Gamma F$.

Пункт 2) есть прямое следствие пункта 1). □

Положим

$$\begin{aligned} S &= \{r_{G,u} \mid G \in R[X],\ u \in [X]\},\\ S^\Gamma &= \{r^\Gamma_{G,U} \mid G \in R[X],\ U \in [\pi, X]\}. \end{aligned} \tag{1.33}$$

Для $\chi \subseteq R[X]$ отображения сечения определим равенствами

$$\begin{aligned} S_\chi &= \{r_{G,u} \mid G \in \chi,\ u \in [X]\},\\ S^\Gamma_\chi &= \{r^\Gamma_{G,U} \mid G \in \chi,\ U \in [\pi, X]\}. \end{aligned} \tag{1.34}$$

В силу предложений 1.19 и 1.33 $\mathfrak{G} = (R[X], \preceq, S)$ и $\mathfrak{G}^\Gamma = (R[X], \preceq^\Gamma, S^\Gamma)$ являются консервативными схемами симплификации.

Более того, имеет место следующее утверждение.

Предложение 1.34. *Схемы симплификации $\mathfrak{G}$ и $\mathfrak{G}^\Gamma$ эквивалентны.*

Доказательство. Докажем сначала следующую лемму.

Лемма 1.35. *Для любых $\chi \subseteq R[X]$ и $F \in R[X]$*

$$S_\chi F \subseteq \widehat{S^\Gamma_\chi} F.$$

(*Здесь множество редукций $\widehat{S^\Gamma_\chi}$ определяется формулой* (1.25).)

Доказательство. Пусть $G \in \chi$ и $u \in [X]$. В обозначениях (1.30) если $G = 0$, или $\|c\| < \|a\|$, или $c = 0$, то $r_{G,u}(F) = F \in \widehat{S^\Gamma_\chi} F$. Остаётся рассмотреть случай, когда $G \neq 0$, $\|c\| \geqslant \|a\|$ и $c \neq 0$.

Пусть $j = \|c\|$ и $i = \|a\|$. Имеем

$$c = \pi^j c_j + \pi^{j+1} c_{j+1} + \ldots + \pi^{n-1} c_{n-1}, \quad c_\alpha \in \Gamma, \quad \alpha \in \overline{j, n-1}.$$

Так как $r_{G,u}(F) = F - (c_j + \pi c_{j+1} + \ldots + \pi^{n-1-j} c_{n-1})\pi^{j-i} u\mathring{G}$, то

$$r_{G,u}(F) = r^\Gamma_{G,\pi^{n-1-i}u} \ldots r^\Gamma_{G,\pi^{j+1-i}u} r^\Gamma_{G,\pi^{j-i}u}(F)$$

и, следовательно, $r_{G,u}(F) \in \widehat{S^\Gamma_\chi} F$. □

Вернёмся к доказательству предложения 1.34. Так как $0 \in N_{\mathfrak{G}}$ и $0 \in N_{\mathfrak{G}^\Gamma}$, то ввиду следствия 1.31 из леммы 1.35 следует, что схема симплификации $\mathfrak{G}$ подчинена $\mathfrak{G}^\Gamma$.

Обратно, покажем, что схема симплификации $\mathfrak{G}^\Gamma$ подчинена $\mathfrak{G}$. Для этого согласно замечанию после предложения 1.30 достаточно доказать, что для любых $\chi \subseteq R[X]$ и $F \in R[X]$

$$\mathrm{Nor}_{\mathfrak{G}^\Gamma_\chi}(F) = 0 \implies \mathrm{Nor}_{\mathfrak{G}_\chi}(F) = 0. \tag{1.35}$$

Пусть $\mathrm{Nor}_{\mathfrak{G}^\Gamma_\chi}(F) = 0$ и $H \in \mathrm{Nor}_{\mathfrak{G}_\chi}(F)$. Тогда $H \in \widehat{S_\chi} F$ и ввиду леммы 1.35 $H \in \widehat{S^\Gamma_\chi} F$. Значит, $\mathrm{Nor}_{\mathfrak{G}^\Gamma_\chi}(H) \subseteq \mathrm{Nor}_{\mathfrak{G}^\Gamma_\chi}(F) = 0$ и, следовательно, $\mathrm{Nor}_{\mathfrak{G}^\Gamma_\chi}(H) = 0$. Если $\chi = \varnothing$, то $H = 0$. Если $\chi \neq \varnothing$, то существует такой полином $G \in \chi$, что $\mathrm{LM}(G)$ делит $\mathrm{LM}(H)$, и, значит, $H = 0$ (поскольку полином H нормален относительно $\mathfrak{G}_\chi$). Итак, $\mathrm{Nor}_{\mathfrak{G}_\chi}(F) = 0$ и импликация (1.35) доказана. □

Несмотря на то, что $\mathfrak{G}$ и $\mathfrak{G}^\Gamma$ эквивалентны, следующее легко доказываемое предложение показывает, что соответствующие множества нормальных полиномов в общем случае различны.

Предложение 1.36. *Пусть даны система $\chi \subseteq R[X]$ и полином $F \in R[X]$, тогда справедливы следующие утверждения*:

1) $F \in N_{\mathfrak{G}_\chi} \iff \mathrm{Supp}(F) \subseteq [\pi, X] \setminus \mathrm{LM}(\chi)[\pi, X]$;
2) $F \in N_{\mathfrak{G}^\Gamma_\chi} \iff \mathrm{Supp}^\Gamma(F) \subseteq [\pi, X] \setminus \mathrm{LM}(\chi)[\pi, X]$.

Пример 1.37. Пусть $R = \mathbb{Z}_4$ и $\Gamma = \{0, 1\}$. Рассмотрим кольцо полиномов $\mathbb{Z}_4[x]$. Пусть $\chi = \{2\}$. Полином $3x$ нормален относительно $\mathfrak{G}_\chi$ и редуцируем относительно $\mathfrak{G}^\Gamma_\chi$, так как $r^\Gamma_{2,x}(3x) = 3x - 2x = x \neq 3x$.

Схемы симплификации $\mathfrak{G}$ и $\mathfrak{G}^\Gamma$ в общем случае не R-линейны (см. определение 1.25), тем не менее имеет место следующее утверждение.

Предложение 1.38 ([2]). *Для любых полинома $G \in R[X] \setminus 0$ и монома $u \in [X]$*

$$r_{G,u} \in \mathrm{End}_R(\pi^{\|G\|} R[X]). \tag{1.36}$$

Из утверждения 1.38 вытекает, что тройка $(\pi^d R[X], \preceq, S_\chi)$, где $d \geqslant \max\{\|G\| \mid G \in \chi\}$, является R-линейной схемой симплификации.

Замечание 1.39. Если $\|G\| = 0$, то $\mathrm{Lc}(G) \in R^*$ и мы можем описать редукцию одной формулой:

$$r_{G,u}(F) = F - \mathrm{Cf}(F, u\,\mathrm{Lm}(G))\,\mathrm{Lc}(G)^{-1} uG. \tag{1.37}$$

Отсюда непосредственно видно, что $r_{G,u} \in \mathrm{End}_R(R[X])$.

Если $\|G\| \neq 0$, то $r_{G,u}$, вообще говоря, не является линейным отображением. Тем не менее для любого элемента $a \in R^*$ имеет место соотношение

$$r_{G,u}(aF) = a r_{G,u}(F). \tag{1.38}$$

1.4. Стандартные базисы и S-полиномы

В этом разделе по аналогии с известными результатами для полиномов над полями (см., например, [5, 12]) вводится понятие S-полинома и на его основе строятся стандартные базисы полиномиального идеала по его произвольной системе образующих.

Зафиксируем некоторый допустимый порядок $\preceq$ на полугруппе мономов $[X]$ и семейство представителей классов вычетов $\Gamma \subseteq R$ $(0 \in \Gamma)$ для $R/\pi R$.

Определение 1.40. Будем говорить, что полином $F \in R[X]$ обладает *представлением относительно системы полиномов* $\chi \subseteq R[X]$, если

$$F = \sum_{i=1}^{m} a_i u_i G_i, \tag{1.39}$$

где $a_i \in R$, $u_i \in [X]$ и $G_i \in \chi$. *Параметром* представления (1.39) назовём π-моном

$$W = \max_{\preceq}\{\mathrm{LM}(a_i u_i G_i) \mid i \in \overline{1,m}\}. \tag{1.40}$$

При $m = 0$ полагаем $W = 0$.

Предложение 1.41 ([2]). *Если полином $F \in R[X]$ обладает представлением* (1.39) *с параметром W, то*

$$\mathrm{LM}(F) \preceq W. \tag{1.41}$$

Определение 1.42. Представление (1.39) называется *H-представлением* (*относительно* χ), если $\mathrm{LM}(F) = W$, где W — параметр этого представления.

Рассмотрим естественное отношение делимости $\mid$ на полугруппе $[X]$. Очевидно, что $([X], \cdot, \mid)$ — упорядоченная полугруппа, изоморфная упорядоченной полугруппе $(\mathbb{N}_0^k, +, \leqslant)$, где $+$ означает покомпонентное сложение, а порядок $\leqslant$ получается из обычного порядка на $\mathbb{N}_0$ по формуле

$$(a_1, \ldots, a_k) \leqslant (b_1, \ldots, b_k) \overset{\text{def}}{\iff} a_1 \leqslant b_1, \ldots, a_k \leqslant b_k. \tag{1.42}$$

Мы можем также рассматривать отношение $\mid$ на $[\pi, X]$. Для любых двух π-мономов $U, V \in [\pi, X]$ существует их точная верхняя грань ($\mathrm{НОК}(U, V)$) и точная нижняя грань ($\mathrm{НОД}(U, V)$), таким образом $([\pi, X], \mid)$ — решётка. Отметим также, что $U \mid V \implies \|U\| \leqslant \|V\|$.

Пусть $F, G \in R[X] \setminus 0$ и $\mathrm{LM}(F) = \pi^a u$, $\mathrm{LM}(G) = \pi^b v$, где $a, b \in \overline{0, n-1}$ и $u, v \in [X]$. Пусть $w = \mathrm{НОД}(u, v) \in [X]$ и $c = \max\{a, b\}$. Существуют такие мономы $u', v' \in [X]$, что $u = wu'$ и $v = wv'$. *S-полиномом* от F и G назовём полином

$$S(F, G) = \pi^{c-a} v' \mathring{F} - \pi^{c-b} u' \mathring{G}. \tag{1.43}$$

Равенство (1.43) можно рассматривать как представление полинома $S(F, G)$ относительно системы $\chi = \{\mathring{F}, \mathring{G}\}$. Параметром этого представления будет π-моном $\pi^c u' v' w$, он называется *начальным параметром* S-полинома $S(F, G)$.

Для удобства полагаем $S(F, 0) = S(0, G) = 0$ для любых полиномов $F, G \in$ $\in R[X]$, причём параметр в этом случае считается равным 0.

Отметим, что для любых полиномов $F, G \in R[X]$ начальный параметр S-полинома равен $\mathrm{НОК}(\mathrm{LM}(F), \mathrm{LM}(G))$.

Определение 1.43. Систему полиномов $\chi \subseteq R[X]$ назовём *π-однородной*, если все полиномы из χ имеют одну и ту же норму.

Любую систему $\chi \subseteq R[X]$ можно представить в виде объединения π-однородных подсистем:

$$\chi = \chi_0 \cup \chi_1 \cup \ldots \cup \chi_t. \tag{1.44}$$

Положим $\alpha_s = \|\chi_s\|$, $s \in \overline{0,t}$. Используя разложение (1.44), всегда будем считать, что

$$0 \leqslant \alpha_0 < \alpha_1 < \ldots < \alpha_t < n. \tag{1.45}$$

В $R[X]$ найдутся такие системы полиномов ψ_s, $s \in \overline{0,t}$, что

$$\pi^{\alpha_s}\psi_s = \chi_s, \quad s \in \overline{0,t}. \tag{1.46}$$

Также для удобства записи положим $\chi_{t+1} = \psi_{t+1} = \varnothing$ и $\alpha_{t+1} = \|\chi_{t+1}\| = n$.

Следующая теорема является аналогом леммы о композиции (см., например, [5, 12]) из теории базисов Грёбнера над полями.

Теорема 1.44. *Пусть χ — непустая система полиномов из идеала I кольца $R[X]$, представленная в виде объединения π-однородных подсистем* (1.44) *со свойством* (1.45), *пусть также выбраны системы полиномов ψ_s, $s \in \overline{0,t+1}$, такие что выполняется условие* (1.46). *Тогда эквивалентны следующие утверждения*:

1) χ — *$\mathfrak{G}$-стандартный базис идеала I*;
1$^\Gamma$) χ — *$\mathfrak{G}^\Gamma$-стандартный базис идеала I*;
2) $\mathrm{LM}(I) = \mathrm{LM}(\chi)[\pi, X]$ — *идеал полугруппы $[\pi, X]$, порождённый* $\mathrm{LM}(\chi)$;
3) *для любого $F \in I$ существует $G \in \chi$, такой что* $\mathrm{LM}(G) \mid \mathrm{LM}(F)$;
4) *любой полином $F \in I$ обладает H-представлением относительно χ*;
5) $I = (\chi)$ *и* $\mathrm{Nor}_{\mathfrak{G}_\chi}(S(G_1, G_2)) = 0$ *для любых* $G_1, G_2 \in \chi$;
5$^\Gamma$) *то же, что и* 5), *только для* $\mathfrak{G}^\Gamma$;
6) $I = (\chi)$ *и* $\mathrm{Nor}_{\mathfrak{G}_\chi}(S(G_1, G_2)) \ni 0$ *для любых* $G_1, G_2 \in \chi$;
6$^\Gamma$) *то же, что и* 6), *только для* $\mathfrak{G}^\Gamma$;
7) $I = (\chi)$ *и для любых* $G_1, G_2 \in \chi$ *либо* $S(G_1, G_2) = 0$, *либо S-полином* $S(G_1, G_2)$ *обладает представлением с параметром, меньшим его начального параметра*;
8) $I = (\chi)$ *и для любого* $j \in \overline{0,t}$ *и любого* $F \in \pi^{\alpha_j} R[X]$ *справедливо*

$$N_1, N_2 \in \mathrm{Nor}_{\mathfrak{G}_{\chi_0 \cup \ldots \cup \chi_j}}(F) \implies$$
$$\implies N_1 - N_2 \in (\pi^{\alpha_{j+1}}\psi_0 \cup \ldots \cup \pi^{\alpha_{j+1}}\psi_j \cup \chi_{j+1} \cup \ldots \cup \chi_t);$$

9) $I = (\chi)$ *и* $\mathfrak{G}^\Gamma_\chi$ — *схема симплификации с канонизацией.*

Доказательство. Эквивалентность условий 1), 2), 3), 4), 5), 6), 7) и 8) была установлена ранее в [2]. Тем не менее для полноты изложения мы приведём здесь всё доказательство.

Эквивалентность 1) $\iff$ 1^Γ) следует из предложения 1.34.

Эквивалентность 2) $\iff$ 3) очевидна.

Докажем импликацию 3) $\implies$ 1). Пусть $F \in I$ и $H \in \mathrm{Nor}_{\mathfrak{G}_\chi}(F)$, тогда $H = 0$. Иначе ввиду пункта 4) полином $H \in I$ был бы редуцируем.

Проверим импликацию 1) $\implies$ 4). Если $F = 0$, то утверждение верно тривиальным образом. Пусть $F \neq 0$. Согласно 1) существует такая последовательность редукций $r_1, \ldots, r_m \in S_\chi$ $(m \geqslant 1)$, что

$$F = F_0 \xmapsto{r_1} F_1 \xmapsto{r_2} \ldots \xmapsto{r_m} F_m = 0, \quad F_0 \succ F_1 \succ \ldots \succ F_m. \tag{1.47}$$

Пусть $r_i = r_{G_i,u_i}$, где $G_i \in \chi$, $u_i \in [X]$ при $i \in \overline{1,m}$. Имеем $F - a_1u_1G_1 - \ldots - a_mu_mG_m = F_m = 0$, что даёт нам представление (1.39) F относительно χ. Остаётся доказать, что параметр этого представления будет равен $\mathrm{LM}(F)$.

Так как для любого $i \in \overline{1,m}$ справедливо $r_i(F_{i-1}) \neq F_{i-1}$, то для любого $i \in \overline{1,m}$ выполнено $\mathrm{LM}(a_iu_iG_i) \preceq \mathrm{LM}(F_{i-1})$. В силу (1.47) имеем $\mathrm{LM}(F_0) \succeq \mathrm{LM}(F_1) \succeq \ldots \succeq \mathrm{LM}(F_{m-1})$.

Значит, для любого $i \in \overline{1,m}$

$$\mathrm{LM}(a_iu_iG_i) \preceq \mathrm{LM}(F).$$

Поэтому параметр W представления (1.39) не превосходит $\mathrm{LM}(F)$ (относительно порядка $\preceq$). Учитывая предложение 1.41, получаем $W = \mathrm{LM}(F)$.

Докажем импликацию 4) $\implies$ 3). Пусть $F \in I$. Если $F = 0$, то $\mathrm{LM}(F) = 0$ делится на $\mathrm{LM}(G)$ для любого $G \in \chi$. Считаем, что $F \neq 0$. Согласно 5) F обладает H-представлением вида (1.39). По определению H-представления имеем

$$\mathrm{LM}(F) = \max\{\mathrm{LM}(a_iu_iG_i) \mid i \in \overline{1,m}\} = \mathrm{LM}(a_{i_0}u_{i_0}G_{i_0}) = \mathrm{LM}(a_{i_0}u_{i_0})\,\mathrm{LM}(G_{i_0}),$$

и, значит, $\mathrm{LM}(G_{i_0}) \mid \mathrm{LM}(F)$.

Импликации 1) $\implies$ 5) и 1^Γ) $\implies$ 5^Γ) следуют из предложения 1.28.

Импликации 5) $\implies$ 6) и 5^Γ) $\implies$ 6^Γ) очевидны.

Импликации 6) $\implies$ 7) и 6^Γ) $\implies$ 7) доказываются аналогично импликации 1) $\implies$ 5).

Докажем имликацию 7) $\implies$ 4). Допустим, условие 4) не выполнено. Тогда существует полином $F \in I \setminus 0$, не имеющий H-представления. Тем не менее ввиду того, что $I = (\chi)$, полином F имеет представление относительно системы χ. Из всех возможных представлений (1.39) полинома F выберем имеющие наименьший параметр $W \in [\pi, X]$, а из отобранных возьмём такое представление, что мощность множества

$$T = \{i \in \overline{1,m} \mid \mathrm{LM}(a_iu_iG_i) = W\} \tag{1.48}$$

минимальна. Так как F не обладает H-представлением, то $\mathrm{LM}(F) \prec W$ и, значит, $|T| \geqslant 2$. Меняя, если необходимо, нумерацию, можно считать, что $1, 2 \in T$. Имеем $W = \mathrm{LM}(a_1u_1G_1) = \mathrm{LM}(a_2u_2G_2)$, поэтому $\mathrm{LM}(G_1) \mid W$ и $\mathrm{LM}(G_2) \mid W$. Значит, $W = UW_0$, где $W_0 = \mathrm{HOK}(\mathrm{LM}(G_1), \mathrm{LM}(G_2))$ и $U \in [\pi, X]$. Существуют

π-мономы $V_1, V_2 \in [\pi, X]$, такие что $W_0 = V_1 \operatorname{LM}(G_1)$, $W_0 = V_2 \operatorname{LM}(G_2)$. Согласно пункту 8) S-полином $S(G_1, G_2) = V_1\mathring{G}_1 - V_2\mathring{G}_2$ обладает представлением

$$V_1\mathring{G}_1 - V_2\mathring{G}_2 = \sum_{i=1}^{m} a_i' u_i' G_i \tag{1.49}$$

с параметром, меньшим исходного параметра W_0 (добавляя в случае необходимости нулевые слагаемые, можно считать, что множества индексов в представлениях (1.39) и (1.49) совпадают), то есть

$$W_0 \succ \max\{\operatorname{LM}(a_i' u_i' G_i) \mid i \in \overline{1,m}\}. \tag{1.50}$$

По предположению существуют такие элементы $r_1 \in R^*$ и $r_2 \in R^*$, что $\operatorname{Lt}(a_1 u_1 G_1) = r_1 W$ и $\mathring{G}_2 = r_2 G_2$. Тогда $\operatorname{Lt}(a_1 u_1 G_1) = r_1 U V_1 \operatorname{LM}(\mathring{G}_1)$ и $a_1 u_1 G_1 = r_1 U V_1 \mathring{G}_1$. Домножив левую и правую части равенства (1.49) на $r_1 U$, получаем

$$a_1 u_1 G_1 - r_1 r_2 U V_2 G_2 = \sum_{i=1}^{m} r_1 a_i' U u_i' G_i. \tag{1.51}$$

Из формул (1.39) и (1.51) следует, что

$$F = r_1 a_1' U u_1' G_1 + (a_2 u_2 + r_1 r_2 U V_2 + r_1 a_2' U u_2') G_2 + \sum_{i=3}^{m} (a_i u_i + r_1 a_i' U u_i') G_i. \tag{1.52}$$

Эта равенство есть представление полинома F, причём, как следует из соотношения (1.50) и выбора разложения (1.39), или параметр этого представления меньше W, или мощность множества T', определяемого аналогично множеству T, будет меньше мощности T. В любом случае приходим к противоречию с минимальностью величин W и $|T|$.

Проверим импликации 3) $\Longrightarrow$ 8) и 4) $\Longrightarrow$ 8). Пусть $\|F\| \geqslant \alpha_j$ и $N_1, N_2 \in \operatorname{Nor}_{\mathfrak{G}_{\chi_0 \cup \ldots \cup \chi_j}}(F)$. Положим $H = N_1 - N_2 \in I$. Ввиду предложения 1.33 имеем $\|N_1\|, \|N_2\| \geqslant \alpha_j$, а значит, и $\|H\| \geqslant \alpha_j$. Покажем, что $\|H\| \geqslant \alpha_{j+1}$. Допустим противное: $\|H\| < \alpha_{j+1}$. Согласно пункту 4) существует такой полином $G \in \chi$, что $\operatorname{LM}(G) \mid \operatorname{LM}(H)$. Так как $\|\operatorname{LM}(H)\| = \|H\| < \alpha_{j+1}$, то $G \in \chi_0 \cup \ldots \cup \chi_j$. По крайней мере один из коэффициентов $\operatorname{Cf}(N_1, \operatorname{Lm}(H))$ и $\operatorname{Cf}(N_1, \operatorname{Lm}(H))$ не равен 0. Пусть $\operatorname{Cf}(N_1, \operatorname{Lm}(H)) \neq 0$. Так как $\|\operatorname{Cf}(N_1, \operatorname{Lm}(H))\| \geqslant \alpha_j$, то полином N_1 можно редуцировать с помощью полинома G, что противоречит его нормальности. Итак, $\|H\| \geqslant \alpha_{j+1}$. Покажем, что

$$H \in (\pi^{\alpha_{j+1}} \psi_0 \cup \ldots \cup \pi^{\alpha_{j+1}} \psi_j \cup \chi_{j+1} \cup \ldots \cup \chi_t). \tag{1.53}$$

Если $H = 0$, то это очевидно. Пусть $H \neq 0$, тогда согласно пункту 5) полином H обладает H-представлением

$$H = \sum_{i=1}^{m} a_i u_i G_i. \tag{1.54}$$

Так как $\operatorname{LM}(H) = \max\{\operatorname{LM}(a_i u_i G_i) \mid i \in \overline{1,m}\}$, то для любого $i \in \overline{1,m}$

$$\|\operatorname{LM}(a_i u_i G_i)\| \geqslant \|\operatorname{LM}(H)\| \geqslant \alpha_{j+1}. \tag{1.55}$$

Значит, для любого $i \in \overline{1,m}$ справедливо $\|a_i\| \geqslant \alpha_{j+1} - \|G_i\|$, что доказывает включение (1.53).

Убедимся, что 8) $\Longrightarrow$ 1). Пусть $F \in I$, тогда, так как $I = (\chi)$, будем иметь

$$F = \sum_{j=0}^{t} \sum_{s=1}^{m_j} a_s^{(j)} u_s^{(j)} G_s^{(j)}, \tag{1.56}$$

где $G_s^{(j)} \in \chi_j$ для любого $s \in \overline{1,m_j}$. Согласно лемме 1.24 существует композиция одношаговых редукций $\rho_0 \in \hat{S}_{\chi_0}$, такая что для любого $s \in \overline{1,m_0}$

$$\rho_0(a_s^{(0)} u_s^{(0)} G_s^{(0)}) \in \mathrm{Nor}_{\mathfrak{G}_{\chi_0}}(a_s^{(0)} u_s^{(0)} G_s^{(0)}). \tag{1.57}$$

Так как $0 \in \mathrm{Nor}_{\mathfrak{G}_{\chi_0}}(a_s^{(0)} u_s^{(0)} G_s^{(0)})$ для любого $s \in \overline{1,m_0}$, то согласно пункту 9) имеем

$$\rho_0(a_s^{(0)} u_s^{(0)} G_s^{(0)}) \in (\pi^{\alpha_1}\psi_0 \cup \chi_1 \cup \ldots \cup \chi_t) \tag{1.58}$$

для любого $s \in \overline{1,m_0}$. С другой стороны,

$$\rho_0(a_s^{(j)} u_s^{(j)} G_s^{(j)}) \equiv a_s^{(j)} u_s^{(j)} G_s^{(j)} \pmod{\pi^{\alpha_1}\psi_0} \tag{1.59}$$

для любых $j \in \overline{1,t}$, $s \in \overline{1,m_j}$. Учитывая предложение 1.38, из соотношений (1.56), (1.58) и (1.59) получаем

$$\rho_0(F) = \sum_{j=0}^{t} \sum_{s=1}^{m_j} \rho_0(a_s^{(j)} u_s^{(j)} G_s^{(j)}) \in (\pi^{\alpha_1}\psi_0 \cup \chi_1 \cup \ldots \cup \chi_t). \tag{1.60}$$

Рассуждая аналогично, находим такую редукцию $\rho_1 \in \hat{S}_{\chi_0 \cup \chi_1}$, что

$$\rho_1\rho_0(F) \in (\pi^{\alpha_2}\psi_0 \cup \pi^{\alpha_2}\psi_1 \cup \chi_2 \cup \ldots \cup \chi_t). \tag{1.61}$$

В итоге мы получим серию редукций $\rho_0, \rho_1, \ldots, \rho_t \in \hat{S}_\chi$, для которой $\rho_t \ldots \rho_1\rho_0(F) = 0$. Значит, условие из пункта 1) выполнено.

Докажем импликацию 3) $\Longrightarrow$ 9). Пусть $F \in R[X]$ и $N_1, N_2 \in \mathrm{Nor}_{\mathfrak{G}_\chi^\Gamma}(F)$. Допустим, что $H = N_1 - N_2 \neq 0$, тогда $\mathrm{LM}(H) = \pi^i u \neq 0$. Поскольку $H \in I$, то согласно 3) существует полином $G \in \chi$, такой что $\mathrm{LM}(G) \mid \mathrm{LM}(H)$. Имеем $\mathrm{LM}(G) = \pi^j v$, где $j \leqslant i$ и $v \mid u$. Так как N_1 и N_2 нормальны относительно $\mathfrak{G}_\chi^\Gamma$, то

$$\mathrm{Cf}(N_\alpha, u) = a_0^\alpha + a_1^\alpha \pi + \ldots + a_{j-1}^\alpha \pi^{j-1},$$

где $\alpha \in \{1,2\}$ и $a_\beta^\alpha \in \Gamma$, $\beta \in \overline{0,j-1}$. Поскольку $\mathrm{Cf}(N_1,u) - \mathrm{Cf}(N_2,u) = \mathrm{Lc}(H)$ и $\|\mathrm{Lc}(H)\| = i \geqslant j$, то согласно предложению 1.16 $a_\beta^1 = a_\beta^2$ для $\beta \in \overline{0,j-1}$. Значит, $\mathrm{Cf}(N_1,u) = \mathrm{Cf}(N_2,u)$ и, следовательно, $\mathrm{Lc}(H) = 0$, что противоречит нашему предположению. Полученное противоречие доказывает, что $N_1 = N_2$ и, следовательно, $\mathfrak{G}^\Gamma$ — схема симплификации с канонизацией.

Проверим импликацию 9) $\Longrightarrow$ 5^Γ). Пусть полиномы $G_1, G_2 \in \chi$ таковы, что существует $H \in \mathrm{Nor}_{\mathfrak{G}_\chi^\Gamma}(S(G_1,G_2))$, $H \neq 0$. Согласно определению S-полинома $S(G_1,G_2) = U\mathring{G}_1 - V\mathring{G}_2$, где $U, V \in [\pi, X]$ и $U\,\mathrm{LM}(G_1) = V\,\mathrm{LM}(G_2)$. Пусть $V = \pi^i v$ и $U = \pi^j u$, тогда $r_{G_1,u}(U\mathring{G}_1) = 0$ и $r_{G_2,v}(U\mathring{G}_1) = S(G_1,G_2)$.

Из этих формул и леммы 1.35 следует, что $0, S(G_1, G_2) \in \widehat{S^{\Gamma}_{\chi}} \cdot U\mathring{G}_1$. Значит, $0, H \in \mathrm{Nor}_{\mathfrak{G}^{\Gamma}_{\chi}}(U\mathring{G}_1)$ и, следовательно, схема симплификации $\mathfrak{G}^{\Gamma}_{\chi}$ не обладает свойством канонизации. □

Теорема 1.44 показывает, что классы $\mathfrak{G}$-стандартных базисов и $\mathfrak{G}^{\Gamma}$-стандартных базисов совпадают. Поэтому в дальнейшем мы будем употреблять термины «стандартный базис» и «стандартная система» без указания схемы симплификации.

Тем не менее, чтобы отличить рассматриваемые здесь стандартные базисы от базисов из [12,14,15,23] (см. замечание после теоремы 1.4), мы говорим, что $\mathfrak{G}$- и $\mathfrak{G}^{\Gamma}$-стандартные базисы *согласованы с нормой* (1.9) *кольца* R.

Замечание 1.45. Ни в определении 1.29, ни в теореме 1.44 не предполагается конечность множества χ. Например, любой идеал I является тривиальным примером собственного стандартного базиса.

Отметим, что согласно определению 1.29 система $\chi = \varnothing$ является стандартным базисом только для нулевого идеала.

Стандартный базис χ произвольного идеала I может содержать 0. Тем не менее система $\chi \setminus 0$ также является стандартным базисом I.

Условия 6) и 7) теоремы 1.44 позволяют построить эффективную процедуру, определяющую, является ли некоторое конечное множество полиномов $\chi \subset R[X]$ стандартной системой. Более того, алгоритм 1.46, формально повторяющий известный алгоритм для полей, вычисляет стандартный базис идеала, заданного конечной системой образующих.

Алгоритм 1.46 ([2]). Вычисление стандартного базиса.

INPUT: $\phi = \{F_1, \ldots, F_s\} \subset R[X]$
OUTPUT: $\chi = \{G_1, \ldots, G_t\}$ — стандартный базис идеала (ϕ)
INITIALIZATION: $\chi := \phi$, $\mathcal{G} = \{(F_i, F_j) \mid 1 \leqslant i < j \leqslant s\}$
WHILE $\mathcal{G} \neq \varnothing$ **DO**
    Выбираем произвольно $(F, G) \in \mathcal{G}$
    $\mathcal{G} := \mathcal{G} \setminus \{(F, G)\}$
    Вычисляем любой элемент $H \in \mathrm{Nor}_{\mathfrak{G}_{\chi}}(S(F, G))$
    IF $H \neq 0$ **THEN**
        $\mathcal{G} := \mathcal{G} \cup \{(U, H) \mid U \in \chi\}$
        $\chi := \chi \cup \{H\}$
    END IF
END WHILE
RETURN χ

Предложение 1.47. *Любой идеал кольца $R[X]$ обладает конечным стандартным базисом.*

Доказательство. Так как кольцо $R[X]$ нётерово, любой его идеал имеет конечную систему образующих. Применяя к этой системе образующих алгоритм 1.46, получаем конечный стандартный базис исходного идеала. □

Замечание 1.48. Роль полугруппы (моноида) $[\pi, X]$ в наших рассмотрениях аналогична роли основного моноида Γ, используемого при построении *градуированных структур* из [13, 20, 24]. Вместе с тем полугруппа $[\pi, X]$ не является полугруппой с сокращением, тогда как моноид Γ, согласно определению градуированной структуры, должен обладать этим свойством. Таким образом, предлагаемая здесь конструкция не покрывается теорией градуированных структур.

1.5. Минимальные и редуцированные стандартные базисы

Зафиксируем некоторый допустимый порядок $\preceq$ на полугруппе мономов $[X]$ и семейство представителей классов вычетов $\Gamma \subseteq R$ $(0, 1 \in \Gamma)$ для $R/\pi R$.

Определение 1.49. Пусть $\mathfrak{S} = (M, \preceq, S)$ — консервативная схема симплификации на M_R (см. определение 1.27). Элемент $m \in M$ назовём $\mathfrak{S}$-*саморедуцированным* или $\mathfrak{S}$-*самонормальным*, если для любой редукции $s \in S_{\{m\}}$ или $sm = m$, или $sm = 0$. В противном случае будем говорить, что m является $\mathfrak{S}$-*саморедуцируемым*.

Согласно определению 1.27 $S_{\{0\}}$ либо пусто, либо содержит только тождественное отображение. Таким образом, 0 является $\mathfrak{S}$-саморедуцированным для любой схемы симплификации $\mathfrak{S}$.

Предложение 1.50. *Для π-унитарного полинома $G \in R[X]$ эквивалентны следующие условия*:

1) G $\mathfrak{G}$-*самонормален*;
2) G $\mathfrak{G}^\Gamma$-*самонормален*;
3) $\operatorname{Supp}(G) \cap \operatorname{LM}(G)[\pi, X] \subseteq \{\operatorname{LM}(G)\}$.

Доказательство. Если $G = 0$, то все три условия выполняются (условие из пункта 3) принимает вид $\varnothing \subseteq \{0\}$). Пусть теперь $G \neq 0$.

Проверим импликацию 1) $\Longrightarrow$ 3). Допустим, что существует π-моном $U \neq \operatorname{LM}(G)$, такой что $U \in \operatorname{Supp}(G) \cap \operatorname{LM}(G)[\pi, X]$. Имеем $U = \pi^a v \operatorname{LM}(G)$, причём $v \in [X] \setminus \{1\}$ и $a \geqslant 1$, поскольку $\operatorname{LM}(G)$ — наибольший элемент в $\operatorname{Supp}(G)$. Значит, $r_{G,v}(G) \notin \{0, G\}$, что противоречит условию 1).

Импликация 2) $\Longrightarrow$ 3) доказывается аналогично импликации 1) $\Longrightarrow$ 3).

Импликации 3) $\Longrightarrow$ 1) и 3) $\Longrightarrow$ 2) очевидны. □

π-унитарные полиномы, удовлетворяющие условиям 1)—3) предложения 1.50, будем называть *самонормальными* (без указания схемы симплификации).

Предложение 1.51. *Имеют место следующие утверждения.*

1. *Пусть полином* $G \in R[X]$ $\mathfrak{G}$*-саморедуцируем* ($\mathfrak{G}^\Gamma$*-саморедуцируем*) *и* $r \in S_{\{G\}}$ ($r \in S^\Gamma_{\{G\}}$) *— такая редукция, что* $r(G) \notin \{0, G\}$. *Тогда* $r(G) = HG$ *для некоторого* $H \in R[X]^*$.
2. *Для любого полинома* $G \in R[X]$ *существуют самонормальный полином* $F \in R[X]$ *и обратимый полином* $H \in R[X]^*$, *такие что* $GH = F$.

Доказательство.

1. Пусть $r = r_{G,u}$, $u \in [X]$. Так как $r(G) \notin \{0, G\}$, то $u \neq 1$ и $\|\operatorname{Cf}(G, u\operatorname{Lm}(G))\| \geqslant \|\operatorname{Lc}(G)\|$. Элемент $b \in R$, такой что $\operatorname{Cf}(G, u\operatorname{Lm}(G)) = b\operatorname{Lc}(G)$, не может быть обратимым (иначе $\operatorname{LM}(G)$ не будет наибольшим элементом в $\operatorname{Supp}(G)$). Значит, $b \in \pi R$, $1 - bu \in R[X]^*$, что и доказывает наше утверждение, так как $r(G) = r_{G,u}(G) = G - buG = (1 - bu)G$.

Рассмотрим теперь случай схемы симплификации $\mathfrak{G}^\Gamma$. Пусть $r = r^\Gamma_{G,U}$, $U \in [\pi, X]$. Так как $r(G) \notin \{0, G\}$, то $U \neq 1$ и $\operatorname{Cf}^\Gamma(G, U\operatorname{LM}(G)) \neq 0$. Так как $\operatorname{LM}(G)$ — наибольший элемент в $\operatorname{Supp}^\Gamma(G)$, то $\|U\| \geqslant 1$ и, следовательно, $1 - \operatorname{Cf}^\Gamma(G, U\operatorname{LM}(G))U \in R[X]^*$.

2. Пусть G есть $\mathfrak{G}$-саморедуцируемый полином, тогда существует такая редукция $r_{G,u}$, что $r_{G,u}(G) \notin \{0, G\}$. Будем производить эти редукции до получения $\mathfrak{G}$-самонормального полинома A. Данный процесс завершится за конечное число шагов, поскольку порядок $\preceq$ из схемы симплификации $\mathfrak{G}$ (см. раздел 1.2) удовлетворяет условию обрыва убывающих цепочек, а редукции приводят к уменьшению полинома относительно этого порядка. Согласно первому утверждению мы будем иметь $A = BG$, где $B \in R[X]^*$. Пусть $\mathring{A} = aA$, $a \in R^*$, тогда согласно предложению 1.50 полиномы $F = aA$ и $H = aB$ удовлетворяют требованиям предложения. □

В частном случае, когда G — полином от одной переменной, пункт 2 предложения 1.51 совпадает с известной теоремой Крулля (см. [16] или [7]).

Пример 1.52. В кольце $\mathbb{Z}_4[x_1, x_2]$ полином $G = x_1x_2 + 1 + 2x_1x_2^2$ является $\mathfrak{G}$-саморедуцируемым, так как $r_{G,x_2}(G) = G - 2x_2G = x_1x_2 + 1 + 2x_2 \neq G$. Полученный полином $r_{G,x_2}(G) = x_1x_2 + 1 + 2x_2 = (1 - 2x_2)G$ самонормален.

Определение 1.53. Пусть $\mathfrak{S} = (M, \preceq, S)$ — консервативная схема симплификации на M_R. Систему элементов $\chi \subseteq M$ назовём $\mathfrak{S}$-*редуцированной*, если для любого элемента $m \in \chi$ выполнены следующие условия:

1) m является $\mathfrak{S}$-самонормальным;
2) m нормален относительно схемы симплификации $\mathfrak{S}_{\chi\setminus\{m\}}$.

В противном случае будем говорить, что система χ является $\mathfrak{S}$-*редуцируемой*.

Замечание 1.54. Пусть конечная система $\psi \subset R[X]$ $\mathfrak{G}$-редуцируема ($\mathfrak{G}^\Gamma$-редуцируема), тогда существует полином $G \in \psi$, который или $\mathfrak{G}$-саморедуцируем ($\mathfrak{G}^\Gamma$-саморедуцируем), или $\mathfrak{G}$-редуцируем ($\mathfrak{G}^\Gamma$-редуцируем) относительно системы $\chi\setminus\{G\}$. Заменив полином G в системе ψ на результат его редуцирования, мы получим новую систему ψ'. Предложение 1.51 показывает, что $\psi' R[X] = \psi R[X]$.

Применив некоторое число раз подобную процедуру, мы получим такую редуцированную систему χ, что $\chi R[X] = \psi R[X]$. Этот процесс завершится за конечное число шагов, поскольку порядок $\preceq$ из схемы симплификации $\mathfrak{G}$ (см. раздел 1.2) удовлетворяет условию обрыва убывающих цепочек, а редукции приводят к уменьшению полинома относительно этого порядка.

Алгоритм 1.55 реализует описанную выше процедуру редуцирования систем полиномов.

Алгоритм 1.55 ([2]). Редуцирование систем полиномов.

INPUT: $\psi = \{F_1, \ldots, F_s\} \subset R[X]$
OUTPUT: $\chi = \{G_1, \ldots, G_t\}$ — $\mathfrak{G}$-редуцированная ($\mathfrak{G}^\Gamma$-редуцированная) система полиномов, такая что $(\chi) = (\psi)$
INITIALIZATION: $\chi := \psi$
START:
FOR EACH $G \in \chi$
  IF G $\mathfrak{G}$-саморедуцируем ($\mathfrak{G}^\Gamma$-саморедуцируем) **THEN**
    Выбираем редукцию $r \in S_{\{G\}}$ ($r \in S^\Gamma_{\{G\}}$),
      такую что $r(G) \notin \{0, G\}$
    $\chi := \chi \setminus \{G\}$, $\chi := \chi \cup \{r(G)\}$
    GOTO START
  END IF
  IF G $\mathfrak{G}$-редуцируем ($\mathfrak{G}^\Gamma$-редуцируем) относительно $\chi \setminus \{G\}$ **THEN**
    Выбираем $H \in \mathrm{Nor}_{\mathfrak{G}_{\chi\setminus\{G\}}}(G)$ ($H \in \mathrm{Nor}_{\mathfrak{G}^\Gamma_{\chi\setminus\{G\}}}(G)$)
    $\chi := \chi \setminus \{G\}$, $\chi := \chi \cup \{H\}$
    GOTO START
  END IF
END FOR
RETURN χ

В дальнейшем нам потребуется следующее утверждение.

Предложение 1.56. *Пусть $\psi \subset R[X]$ — конечная система полиномов с попарно различными ведущими π-мономами и множество $\mathrm{LM}(\psi)$ является антицепью относительно порядка делимости. Если χ есть результат приведения ψ к $\mathfrak{G}$-редуцированному ($\mathfrak{G}^\Gamma$-редуцированному) виду с помощью алгоритма* 1.55*, то тогда $|\psi| = |\chi|$ и $\mathrm{LM}(\psi) = \mathrm{LM}(\chi)$.*

Доказательство. При саморедуцировании мы заменяем полином G на $r(G) = HG$, $H \in R[X]^*$ (предложение 1.51, 1)). Следовательно, $\mathrm{LM}(r(G)) =$

$= \mathrm{LM}(H)\,\mathrm{LM}(G) = \mathrm{LM}(G)$. При редуцировании G относительно $\chi \setminus \{G\}$ ведущий π-моном $\mathrm{LM}(G)$ не затрагивается, поскольку $\mathrm{LM}(\psi)$ является антицепью. □

Определение 1.57. Пусть $\mathfrak{S} = (M, \preceq, S)$ — консервативная схема симплификации на M_R. $\mathfrak{S}$-стандартный базис χ подмодуля $A \leqslant M_R$ назовём *минимальным*, если никакая собственная часть χ не является $\mathfrak{S}$-стандартным базисом A.

$\mathfrak{S}$-стандартный базис χ подмодуля $A \leqslant M_R$ назовём *$\mathfrak{S}$-редуцированным*, если множество χ является $\mathfrak{S}$-редуцированной (см. определение 1.53) системой и $0 \notin \chi$.

Поскольку согласно теореме 1.44 классы $\mathfrak{G}$- и $\mathfrak{G}^\Gamma$-стандартных базисов совпадают, понятие минимального базиса идеала не зависит от выбора схемы симплификации $\mathfrak{G}$ или $\mathfrak{G}^\Gamma$. Поэтому в дальнейшем мы будем употреблять термин *минимальный стандартный базис* без указания схемы симплификации.

Пусть $(M, \preceq)$ — упорядоченное множество. Совокупность минимальных элементов M относительно $\preceq$ будем обозначать $\min(M, \preceq)$. Ясно, что для любого упорядоченного множества $(M, \preceq)$ совокупность $\min(M, \preceq)$ будет антицепью.

Определение 1.58. *Множеством обструкций* идеала $I \lhd R[X]$ называется совокупность π-мономов

$$O(I) = \min(\mathrm{LM}(I), |). \tag{1.62}$$

Отметим, что множество обструкций неявно зависит от выбора допустимого порядка на $[X]$, так как от этого выбора зависит $\mathrm{LM}(I)$.

Предложение 1.59 ([2]).

1. *Упорядоченное множество* $([\pi, X], |)$ *конечно свободно* (*то есть оно содержит лишь конечные антицепи*).
2. *Полугруппа* $[\pi, X]$ *нётерова* (*то есть любой её полугрупповой идеал конечно порождён*).

Так как отношение делимости удовлетворяет условию минимальности, то $O(I)$ всегда непусто. Более того, $O(I)$ — антицепь в $([\pi, X], |)$, и, следовательно, согласно предложению 1.59 $O(I)$ всегда конечно.

Лемма 1.60. *Пусть I — идеал в $R[X]$ и χ — стандартный базис идеала I. Тогда $\mathfrak{G}_I^\Gamma$ и $\mathfrak{G}_\chi^\Gamma$ — схемы симплификации с канонизацией и*

$$\mathrm{Can}_{\mathfrak{G}_I^\Gamma} = \mathrm{Can}_{\mathfrak{G}_\chi^\Gamma}. \tag{1.63}$$

Доказательство. Первое утверждение следует из теоремы 1.44 и того, что множества I и χ являются стандартными базисами I.

Докажем равенство (1.63). Пусть $F \in R[X]$, тогда согласно предложению 1.36 полиномы $\mathrm{Can}_{\mathfrak{G}_I^\Gamma}(F)$ и $\mathrm{Can}_{\mathfrak{G}_\chi^\Gamma}(F)$ нормальны относительно $\mathfrak{G}_\chi^\Gamma$. Используя те же рассуждения, что и при доказательстве импликации $4) \implies 9)$ из теоремы 1.44, находим, что $\mathrm{Can}_{\mathfrak{G}_I^\Gamma}(F) = \mathrm{Can}_{\mathfrak{G}_\chi^\Gamma}(F)$. □

Лемма 1.60 показывает, что отображение $\mathrm{Can}_{\mathfrak{G}_\chi^\Gamma}$ не зависит от выбора стандартного базиса χ идеала I.

Теорема 1.61. *Пусть I — ненулевой идеал в $R[X]$, тогда имеют место следующие утверждения.*

1. *Система $\chi \subseteq I$ является стандартным базисом I, если и только если $O(I) \subseteq \mathrm{LM}(\chi)$.*
2. *Стандартный базис χ идеала I минимален в том и только том случае, когда $|\chi| = |O(I)|$.*
3. *Любой $\mathfrak{G}$-редуцированный стандартный базис является минимальным.*
4. *Любой $\mathfrak{G}^\Gamma$-редуцированный стандартный базис является $\mathfrak{G}$-редуцированным.*
5. *Идеал I обладает единственным $\mathfrak{G}^\Gamma$-редуцированным стандартным базисом, состоящим из π-унитарных полиномов.*

Доказательство. Утверждения 1—3 доказаны в [2, теорема 3]. Утверждение 4 следует из леммы 1.35.

Докажем утверждение 5. Из произвольного стандартного базиса χ идеала I (например, можно положить $\chi = I$) получим минимальный стандартный базис, выбрав из χ для каждого $U \in O(I)$ ровно по одному полиному с ведущим π-мономом, равным U (см. 1 и 2). Применив к найденному базису алгоритм 1.55, получим $\mathfrak{G}^\Gamma$-редуцированный стандартный базис идеала I. Заменяя в этом базисе каждый полином G на $\mathring{G}$, получим искомый базис.

Докажем единственность. Пусть χ и ψ — $\mathfrak{G}^\Gamma$-редуцированные стандартные базисы идеала I, состоящие из π-унитарных полиномов. Пусть полиномы $F \in \chi$ и $G \in \phi$ таковы, что $\mathrm{LM}(F) = \mathrm{LM}(G) = U$. Имеют место следующие представления: $F = U - F_0$ и $G = U - G_0$. Согласно лемме 1.60 имеем

$$F_0 = \mathrm{Can}_{\mathfrak{G}^\Gamma_\chi}(U) = \mathrm{Can}_{\mathfrak{G}^\Gamma_\psi}(U) = G_0,$$

и, следовательно, $F = G$. □

Следующее предложение показывает, насколько однозначно определены параметры минимальных и $\mathfrak{G}$-редуцированных стандартных базисов. Отметим, что аналогичные утверждения были доказаны ранее для канонической системы образующих (см. [7, 9, 10]).

Предложение 1.62 ([2]). *Пусть $\chi = \chi_0 \cup \ldots \cup \chi_t$ и $\phi = \phi_0 \cup \ldots \cup \phi_s$ — минимальные стандартные базисы идеала I, представленные в виде* (1.44) *со свойством* (1.45). *Тогда $t = s$, $|\chi_i| = |\phi_i|$ и $\|\chi_i\| = \|\phi_i\| = \alpha_i$, $i \in \overline{0,t}$.*

Если, кроме того, стандартные базисы χ и ϕ являются $\mathfrak{G}$-редуцированными, то $\chi_i \equiv \phi_i (I \cap \pi^{\alpha_{i+1}} R[X])$, $i \in \overline{0,t}$.

Пример 1.63. Отметим, что, в отличие от $\mathfrak{G}^\Gamma$-редуцированного стандартного базиса, $\mathfrak{G}$-редуцированный стандартный базис определяется, вообще говоря, неоднозначно. Например, для $R[X] = \mathbb{Z}_4[x_1]$ системы полиномов $\{x_1^2 + x_1, 2x_1\}$ и $\{x_1^2 + 3x_1, 2x_1\}$ являются редуцированными стандартными базисами одного и того же идеала и только первая из них есть $\mathfrak{G}^\Gamma$-редуцированный стандартный базис (при $\Gamma = \{0, 1\}$).

2. Стандартные базисы и вычисления в идеалах

2.1. Основные свойства стандартных базисов

Зафиксируем некоторый допустимый порядок $\preceq$ на полугруппе мономов $[X]$ и семейство представителей классов вычетов $\Gamma \subseteq R$ $(0 \in \Gamma)$.

Пусть даны идеал $I \lhd R[X]$, порождённый системой полиномов $\psi = \{F_1, \ldots, F_l\}$, и полином $F \in R[X]$. Рассматриваемые стандартные базисы позволяют определить, лежит полином F в идеале I или нет (*проблема вхождения*), и, если лежит, найти полиномы $H_1, \ldots, H_l \in R[X]$, такие что

$$F = H_1F_1 + \ldots + H_lF_l. \tag{2.1}$$

А именно, пусть $\chi = \{G_1, \ldots, G_m\}$ — стандартный базис идеала $I = \psi R[X]$. С помощью последовательного редуцирования вычислим какой-нибудь полином $L \in \mathrm{Nor}_{\mathfrak{G}_\chi}(F)$. Тогда согласно определению 1.29

$$F \in I \iff L = 0.$$

Пусть $L = 0$, тогда $F = K_1G_1 + \ldots + K_mG_m$, при этом полиномы K_i, $i \in \overline{1,m}$, могут быть получены в процессе редуцирования F. Существует матрица $T_{l\times m}$ с коэффициентами из $R[X]$, такая что

$$(G_1, \ldots, G_m) = (F_1, \ldots, F_l)T.$$

Матрица T может быть построена при вычислении стандартного базиса χ, для этого на каждом шаге алгоритма 1.46 нужно сохранять соответствующую информацию о редукциях.

Вектор

$$(H_1, \ldots, H_l) = (K_1, \ldots, K_m)T^t$$

представляет собой искомый набор коэффициентов в разложении (2.1) (здесь символ ^{t} означает взятие транспонированной матрицы).

Пусть идеалы I и J заданы конечными системами порождающих. Ясно, что алгоритм, решающий проблему вхождения, позволяет также определять, выполняются ли соотношения $I \subseteq J$ и $I = J$.

Отметим, что все описанные выше задачи могут быть решены с помощью стандартных базисов из [12, 14, 23].

Следующей важной задачей является определение системы представителей классов вычетов $R[X]$ по идеалу I. Мы рассмотрим более общий случай.

Предложение 2.1. *Пусть даны идеалы $I, J \lhd R[X]$, такие что $I \subseteq J$, и пусть G_U, $U \in \mathrm{LM}(J) \setminus \mathrm{LM}(I)$, — система полиномов из J, таких что $\mathrm{Lt}(G_U) = U$. Тогда множество полиномов вида*

$$\sum_{U\in \mathrm{LM}(J)\setminus \mathrm{LM}(I)} a_U G_U \tag{2.2}$$

(*где лишь конечное число коэффициентов $a_U \in \Gamma$ отлично от* 0) *образует систему представителей классов вычетов J по I.*

Доказательство. Пусть H — некоторый ненулевой полином из J, такой что $\mathrm{Supp}^{\Gamma}(H) \subseteq [\pi, X] \setminus \mathrm{LM}(I)$. Тогда $\mathrm{LM}(H) \in \mathrm{LM}(J) \setminus \mathrm{LM}(I)$. Пусть $a = \mathrm{Cf}^{\Gamma}(H, \mathrm{LM}(H)) \in \Gamma$, положим

$$\tilde{H} = \mathrm{Can}_{\mathfrak{G}_I^{\Gamma}}(H - aG_{\mathrm{LM}(H)}).$$

Ясно, что полином $\tilde{H}$ лежит в J, $\mathrm{Supp}^{\Gamma}(H) \subseteq [\pi, X] \setminus \mathrm{LM}(I)$ и $\mathrm{LM}(\tilde{H}) \prec \mathrm{LM}(H)$.

Пусть теперь $F \in J$, положим $F_0 = \mathrm{Can}_{\mathfrak{G}_I^{\Gamma}}(F)$. Предположим, что полином F_i, $i \geqslant 0$, уже построен. Если $F_i = 0$, заканчиваем построение, иначе полагаем $F_{i+1} = \tilde{F}_i$. Этот процесс обязательно оборвётся, поскольку

$$\mathrm{LM}(F_0) \succ \mathrm{LM}(F_1) \succ \ldots.$$

Значит, найдётся такой номер $m \in \mathbb{N}_0$, что $F_0, \ldots, F_{m-1}$ не равны 0, а F_m равен 0. Имеем

$$0 = F_m \overset{I}{\equiv} F_{m-1} - \mathrm{Cf}^{\Gamma}(F_{m-1}, \mathrm{LM}(F_{m-1}))G_{\mathrm{LM}(F_{m-1})} \overset{I}{\equiv} \ldots \overset{I}{\equiv}$$
$$\overset{I}{\equiv} F_0 - \sum_{i=0}^{m-1} \mathrm{Cf}^{\Gamma}(F_i, \mathrm{LM}(F_i))G_{\mathrm{LM}(F_i)}$$

(символ $\overset{I}{\equiv}$ означает равенство по модулю идеала I), и, следовательно,

$$F \overset{I}{\equiv} \sum_{i=0}^{m-1} \mathrm{Cf}^{\Gamma}(F_i, \mathrm{LM}(F_i))G_{\mathrm{LM}(F_i)}.$$

Докажем теперь, что при различных a_U полиномы (2.2) попарно несравнимы по модулю I. Допустим

$$\sum_{i=1}^{l} a_i G_{U_i} \overset{I}{\equiv} \sum_{i=1}^{l} b_i G_{U_i}, \tag{2.3}$$

где $U_1 \prec \ldots \prec U_l$ — π-мономы из $\mathrm{LM}(J) \setminus \mathrm{LM}(I)$ и $a_i, b_i \in \Gamma$, $i \in \overline{1,l}$. Если $a_l - b_l \in R^*$, то ведущий π-моном разности левой и правой части сравнения (2.3) будет равен $\mathrm{LM}(G_{U_l}) = U_l$, что невозможно, поскольку $U_l \notin \mathrm{LM}(I)$. Значит, $a_l - b_l \in \pi R$ и, следовательно, $a_l = b_l$. Рассуждая аналогично, докажем, что $a_i = b_i$, $i \in \overline{1,l}$. □

Из доказательства предложения 2.1 видно, что для полинома $F \in J$ представитель класса вычетов $F + I$ вида (2.2) может быть эффективно вычислен.

Из предложения 2.1 легко получить следующие три следствия.

Следствие 2.2. *Для идеала $I \lhd R[X]$ множество полиномов вида*

$$\sum_{U \in [\pi, X] \setminus \mathrm{LM}(I)} a_U U$$

(*где лишь конечное число коэффициентов $a_U \in \Gamma$ отлично от* 0) *образует систему представителей классов вычетов $R[X]$ по I.*

Следствие 2.3. *Пусть поле вычетов $\bar{R}$ конечно и идеалы $I, J \lhd R[X]$ таковы, что $I \subseteq J$. Тогда модуль J/I конечен, если и только если множество $\mathrm{LM}(J) \setminus \mathrm{LM}(I)$ конечно, причём в этом случае*

$$|J/I| = |\bar{R}|^{|\,\mathrm{LM}(J)\setminus\mathrm{LM}(I)|}. \tag{2.4}$$

Отметим, что при $J = R[X]$ и унитарном I формула (2.4) была получена ранее в [17].

Следствие 2.4. *Пусть даны идеалы $I, J \lhd R[X]$, такие что $I \subseteq J$ и $\pi J \subseteq I$. Тогда полиномы G_U, выбираемые так же, как и в предложении* 2.1, *образуют базис $(J/I)_{\bar{R}}$ (с естественной структурой $\bar{R}$-пространства). И значит, в частности,*

$$\dim(J/I)_{\bar{R}} = |\,\mathrm{LM}(J) \setminus \mathrm{LM}(I)|.$$

Заметим, что ввиду пункта 3) теоремы 1.44 параметр $|\,\mathrm{LM}(J) \setminus \mathrm{LM}(I)|$, фигурирующий в предыдущих двух следствиях, может быть эффективно вычислен исходя из стандартных базисов идеалов I и J.

В следующем предложении устанавливаются свойства стандартных базисов, аналогичные свойствам канонической системы образующих из [10] (см. [10, теорема 4.11]).

Предложение 2.5 ([2]). *Пусть $\chi = \chi_0 \cup \ldots \cup \chi_t$ — стандартный базис идеала I, представленный в виде* (1.44) *со свойством* (1.45). *Выберем системы полиномов ψ_s, $s \in \overline{0, t+1}$, так, чтобы выполнялось условие* (1.46). *Пусть также задано число $a \in \overline{0, n}$ и $j_0 = \min\{j \in \overline{0, t+1} \mid a \leqslant \alpha_j\}$. Тогда справедливы следующие утверждения*:

1) $\chi_0 \cup \ldots \cup \chi_{j_0-1} \cup \{\pi^a\}$ — *стандартный базис идеала $I + \pi^a R[X]$*;
2) $\psi_0 \cup \ldots \cup \psi_{j_0-1} \cup \pi^{\alpha_{j_0}-a}\psi_{j_0} \cup \ldots \cup \pi^{\alpha_t-a}\psi_t \cup \{\pi^{n-a}\}$ — *стандартный базис идеала $(I : \pi^a)$*;
3) $\pi^a\psi_0 \cup \ldots \cup \pi^a\psi_{j_0-1} \cup \chi_{j_0} \cup \ldots \cup \chi_t$ — *стандартный базис идеала $I \cap \pi^a R[X]$.*

2.2. Модуль сизигий и вычисления в идеалах

В этом разделе мы доказываем теорему о порождающих модуля сизигий системы полиномов из $R[X]$ и с её помощью решаем ряд алгоритмических задач об идеалах в $R[X]$.

Здесь и в дальнейшем элементы свободного $R[X]$-модуля $R[X]^d$, $d \in \mathbb{N}$, мы записываем как строки длины d. Система векторов

$$\boldsymbol{e}_1 = (1, 0, \ldots, 0),\ \boldsymbol{e}_2 = (0, 1, \ldots, 0), \ldots,\ \boldsymbol{e}_d = (0, 0, \ldots, 1)$$

образует базис $R[X]^d_{R[X]}$.

Определение 2.6. *Модулем сизигий* системы полиномов $F_1, \ldots, F_l \in R[X]$ называется множество

$$\mathrm{Syz}(F_1, \ldots, F_l) = \{(H_1, \ldots, H_l) \in R[X]^l \mid F_1H_1 + \ldots + F_lH_l = 0\}. \tag{2.5}$$

Очевидно, что $\mathrm{Syz}(F_1,\dots,F_l)$ является $R[X]$-подмодулем в $R[X]^l$.

Пусть $G_1,\dots,G_m \in R[X]$ образуют стандартную систему π-унитарных полиномов. Тогда согласно теореме 1.44 для любых $i,j \in \overline{1,m}$, $i \neq j$, S-полином $S(G_i,G_j) = V_{ij}G_i - U_{ij}G_j$ обладает H-представлением относительно системы полиномов $\chi = \{G_1,\dots,G_m\}$, а именно

$$V_{ij}G_i - U_{ij}G_j = \sum_{\alpha=1}^{m}\Bigl(\sum_{k=1}^{m_\alpha} a_{ij\alpha}^k u_{ij\alpha}^k\Bigr)G_\alpha,$$

где $a_{ij\alpha}^k \in R$, $u_{ij\alpha}^k \in [X]$ и $\mathrm{LM}(a_{ij\alpha}^k u_{ij\alpha}^k G_\alpha) \preceq \mathrm{LM}(S(G_i,G_j))$. Вектор

$$\boldsymbol{s}_{ij} = V_{ij}\boldsymbol{e}_i - U_{ij}\boldsymbol{e}_j - \sum_{\alpha=1}^{m}\Bigl(\sum_{k=1}^{m_\alpha} a_{ij\alpha}^k u_{ij\alpha}^k\Bigr)\boldsymbol{e}_\alpha \in R[X]^m \tag{2.6}$$

назовём *S-сизигией*.

Пусть также

$$\boldsymbol{p}_k = \pi^{n-\|G_k\|}\boldsymbol{e}_k \in R[X]^m. \tag{2.7}$$

Вектор $\boldsymbol{p}_k$, $k \in \overline{1,m}$, назовём π-сизигией. Очевидно, что $\boldsymbol{s}_{ij}, \boldsymbol{p}_k \in \mathrm{Syz}(G_1,\dots,G_m)$.

Теорема 2.7. *Пусть $G_1,\dots,G_m \in R[X]$ образуют стандартную систему π-унитарных полиномов. Тогда модуль сизигий $\mathrm{Syz}(G_1,\dots,G_m)$ порождается системой векторов $\{\boldsymbol{s}_{ij} \mid i,j \in \overline{1,m},\ i \neq j\} \cup \{\boldsymbol{p}_k \mid k \in \overline{1,m}\}$.*

Доказательство. Пусть N — $R[X]$-подмодуль в $R[X]^m$, порождённый S-сизигиями и π-сизигиями. Ясно, что $N \subseteq \mathrm{Syz}(G_1,\dots,G_m)$. Предположим, что $N \neq \mathrm{Syz}(G_1,\dots,G_m)$. Выберем сизигии $\boldsymbol{r} = (R_1,\dots,R_m) \in \mathrm{Syz}(G_1,\dots,G_m)\backslash N$, такие что π-моном $\max\{\mathrm{LM}(R_iG_i) \mid i \in \overline{1,m}\}$ имеет наименьшее возможное значение W, а из отобранных возьмём такую сизигию, что мощность множества

$$T = \{i \in \overline{1,m} \mid \mathrm{LM}(R_iG_i) = W\} \tag{2.8}$$

минимальна. Так как N содержит π-сизигии, то $W \neq 0$ и, значит, $|T| \geqslant 2$. Пусть $i,j \in T$, $i \neq j$. Имеем $W = \mathrm{LM}(R_iG_i) = \mathrm{LM}(R_jG_j)$, поэтому $\mathrm{LM}(G_i) \mid W$ и $\mathrm{LM}(G_j) \mid W$. Значит, $W = UW_0$, где $W_0 = \mathrm{HOK}(\mathrm{LM}(G_i),\mathrm{LM}(G_j))$ и $U \in [\pi,X]$.

Существует такой элемент $b \in R^*$, что $\mathrm{Lt}(R_iG_i) = bW$. Очевидно, что сизигия $\boldsymbol{r}' = \boldsymbol{r} - bU\boldsymbol{s}_{ij}$ принадлежит $\mathrm{Syz}(G_1,\dots,G_m) \setminus N$. Параметры W' и T' этой сизигии, определяемые аналогично W и T, таковы, что или $W' \prec W$, или $W' = W$ и $|T'| < |T|$. В любом случае приходим к противоречию с минимальностью величин W и $|T|$. □

Пусть теперь $\psi = \{F_1,\dots,F_l\} \subset R[X]$ — произвольная система полиномов, и пусть $G_1,\dots,G_m$ — стандартный базис идеала $\psi R[X]$, состоящий из π-унитарных полиномов. Существуют такие матрицы $T_{l\times m}$ и $S_{m\times l}$ с коэффициентами из $R[X]$, что

$$(F_1,\dots,F_l) = (G_1,\dots,G_m)S \quad \text{и} \quad (G_1,\dots,G_m) = (F_1,\dots,F_l)T.$$

Предложение 2.8 ([12]). *Модуль сизигий* $\mathrm{Syz}(F_1,\dots,F_l)$ *порождается столбцами матрицы* $E_l - TS$ *и векторами вида* $T\boldsymbol{s}_{ij}^t$, $T\boldsymbol{p}_k^t$, $i,j,k \in \overline{1,m}$, $i \neq j$, *где* E_l *— единичная матрица размера* $l \times l$, *а* $\boldsymbol{s}_{ij}$ *и* $\boldsymbol{p}_k$ *— S-сизигии и* π*-сизигии для* $G_1,\dots,G_m$.

Отметим, что матрица S из предложения 2.8 может быть найдена при редуцировании полиномов F_i относительно стандартного базиса $\{G_1,\dots,G_m\}$. Матрица T может быть построена при вычислении стандартного базиса $\{G_1,\dots,G_m\}$, для этого на каждом шаге нужно сохранять соответствующую информацию о редукциях.

Как и в классическом случае над полями, сизигии позволяют решать многие вычислительные задачи в идеалах.

Пусть I и J — идеалы в $R[X]$, и пусть $F_1,\dots,F_l$ и $G_1,\dots,G_m$ — системы порождающих для I и J соответственно. Пусть модуль сизигий

$$\mathrm{Syz}(F_1,\dots,F_l,G_1,\dots,G_m)$$

порождается системой векторов $\{\boldsymbol{H}_\alpha = (H_\alpha^1,\dots,H_\alpha^{l+m}) \mid \alpha \in \overline{1,s}\}$, тогда идеал $I \cap J$ будет порождаться системой полиномов

$$F_1 H_\alpha^1 + \ldots + F_l H_\alpha^l, \quad \alpha \in \overline{1,s}.$$

Частным идеалов I и J называется идеал

$$I : J = \{H \in R[X] \mid JH \subseteq I\}.$$

Имеет место равенство

$$I : J = \bigcap_{i=1}^{m} (I : G_i R[X]).$$

Таким образом, задача построения системы порождающих идеала $I : J$ сводится к нахождению порождающих идеалов вида $I : GR[X]$.

Рассмотрим модуль сизигий $\mathrm{Syz}(F_1,\dots,F_l,G)$. Пусть он порождается системой векторов $\{\boldsymbol{H}_\alpha = (H_\alpha^1,\dots,H_\alpha^{l+1}) \mid \alpha \in \overline{1,s}\}$. Тогда идеал $I : GR[X]$ порождается полиномами

$$H_\alpha^{l+1}, \quad \alpha \in \overline{1,s}.$$

2.3. Элиминация

Пусть даны два множества переменных $X = \{x_1,\dots,x_k\}$ и $Y = \{y_1,\dots,y_l\}$. Пусть также дан идеал $I \lhd R[X,Y] = R[x_1,\dots,x_k;y_1,\dots,y_l]$. Задача *элиминации* состоит в нахождении множества порождающих идеала $I_X = I \cap R[X] \lhd R[X]$ исходя из множества порождающих идеала I.

Продолжим естественным образом канонический эпиморфизм $\nu\colon R \to \bar{R}$ до эпиморфизма $\nu\colon R[X,Y]^d \to \bar{R}[X,Y]^d$.

Имеет место следующее очевидное утверждение.

Предложение 2.9. *Пусть в свободном $R[X,Y]$-модуле $R[X,Y]^d$ задан некоторый подмодуль K, и пусть $\boldsymbol{g}_1,\ldots,\boldsymbol{g}_l$ — система векторов из $\bar{R}[X]^d$, порождающая $\bar{R}[X]$-модуль $\bar{K}\cap\bar{R}[X]^d$. Тогда если векторы $\boldsymbol{G}_1,\ldots,\boldsymbol{G}_l$ из $R[X]^d$ таковы, что*

$$\bar{\boldsymbol{G}}_i=\boldsymbol{g}_i,\quad i\in\overline{1,l},$$

то $R[X]$-модуль $(K+\pi R[X,Y]^d)\cap R[X]$ порождается системой векторов

$$\boldsymbol{G}_1,\ldots,\boldsymbol{G}_l,\pi\boldsymbol{e}_1,\ldots,\pi\boldsymbol{e}_d.$$

Предложение 2.9 показывает, что множество $R[X]$-порождающих модуля $(K+\pi R[X,Y])\cap R[X]$ может быть эффективно построено исходя из системы $R[X,Y]$-порождающих модуля K с помощью классических методов элиминации для полей (см., например, [12]).

Пусть идеал $I\lhd R[X,Y]$ задан семейством порождающих $\psi=\{F_1,\ldots,F_l\}\subseteq\subseteq R[X,Y]$. Мы последовательно построим семейства χ_i, $i\in\overline{0,n}$, полиномов из $R[X]$, такие что

$$(I+\pi^iR[X,Y])\cap R[X]=\chi_iR[X],\quad i\in\overline{0,n}. \tag{2.9}$$

Ясно, что $\chi=\chi_n$ будет искомой системой порождающих идеала $I_X=I\cap R[X]$.

Полагаем $\chi_0=\{1\}$ (мы считаем $\pi^0=1$). Пусть система $\chi_i=\{G_1^i,\ldots,G_{m_i}^i\}$, $i\in\overline{0,n-1}$, уже найдена, построим систему χ_{i+1}.

Рассмотрим модуль сизигий $\mathrm{Syz}(G_1^i,\ldots,G_{m_i}^i,F_1,\ldots,F_l,\pi^{i+1})$ и вычислим (см. раздел 2.2) его систему $R[X,Y]$-порождающих

$$\boldsymbol{H}^\alpha=(H_1^\alpha,\ldots,H_{m_i+l+1}^\alpha),\quad\alpha\in\overline{1,s_i}.$$

Пусть K_i — проекция указанного модуля сизигий на первые m_i координат. Ясно, что $R[X,Y]$-модуль K_i будет порождаться системой векторов $\{(H_1,\ldots,H_{m_i})\mid\alpha\in\overline{1,s_i}\}$. Используя предложение 2.9 и методы элиминации для полей, построим семейство $R[X]$-порождающих

$$\boldsymbol{D}^\alpha=(D_1^\alpha,\ldots,D_{m_i}^\alpha),\quad\alpha\in\overline{1,t_i},$$

модуля $(K_i+\pi R[X,Y]^d)\cap R[X]$.

Предложение 2.10. *Во введённых выше обозначениях семейство полиномов*

$$\chi_{i+1}=\{G_1^iD_1^\alpha+\ldots+G_{m_i}^iD_{m_i}^\alpha\mid\alpha\in\overline{1,t_i}\}\subseteq R[X]$$

удовлетворяет условию (2.9).

Доказательство. Существуют векторы $\boldsymbol{L}^\alpha=(L_1^\alpha,\ldots,L_{m_i}^\alpha)\in K_i$ и $\boldsymbol{T}^\alpha=(T_1^\alpha,\ldots,T_{m_i}^\alpha)\in R[X,Y]^{m_i}$, такие что

$$\boldsymbol{D}^\alpha=\boldsymbol{L}^\alpha+\pi\boldsymbol{T}^\alpha,\quad\alpha\in\overline{1,t_i},$$

и, следовательно,

$$\sum_{j=1}^{m_i}G_j^iD_j^\alpha=\sum_{j=1}^{m_i}G_j^iL_j^\alpha+\sum_{j=1}^{m_i}\pi G_j^iT_j^\alpha.$$

Значит, согласно определению K_i и ввиду соотношения (2.9) для χ_i семейство χ_{i+1} содержится в $(I + \pi^{i+1}R[X,Y]) \cap R[X]$.

Наоборот, пусть $F \in (I + \pi^{i+1}R[X,Y]) \cap R[X]$. Тогда $F \in \chi_i R[X]$ и, следовательно, существуют полиномы $A_1, \ldots, A_{m_i} \in R[X]$ и $B_1, \ldots, B_{l+1} \in R[X,Y]$, такие что

$$F = G_1^i A_1 + \ldots + A_{m_i} G_{m_i}^i = F_1 B_1 + \ldots + F_l B_l + \pi^{i+1} B_{l+1}.$$

Значит, согласно определению модуля K_i вектор $(A_1, \ldots, A_{m_i})$ принадлежит $(K_i + \pi R[X,Y]^d) \cap R[X]$, откуда следует, что $F \in \chi_{i+1} R[X]$. □

С помощью элиминации, как и в классическом случае, можно решить некоторые вычислительные задачи в идеалах. Например, пусть даны идеалы $I_\alpha \lhd R[X]$, $\alpha \in \overline{1,l}$. Введём новые переменные $Y = \{y_1, \ldots, y_l\}$ и рассмотрим идеал K в $R[X,Y]$, порождённый множеством полиномов

$$\{1 - y_1 - \ldots - y_l\} \cup y_1 I_1 \cup \ldots \cup y_l I_l.$$

Тогда

$$I_1 \cap \ldots \cap I_l = K \cap R[X].$$

Вместе с тем следует ожидать, что методы вычисления с помощью сизигий (см. раздел 2.2), как и в классическом случае полиномиальных идеалов над полями, предпочтительнее, с вычислительной точки зрения, методов, основанных на элиминации.

3. Приложения стандартных базисов

3.1. Критерий цикличности ЛРП-семейства

Пусть B — кольцо и M_B — правый B-модуль. Любая функция

$$\mu \colon \mathbb{N}_0^k \to M$$

называется *k-последовательностью* над модулем M_B. Мы пишем $\mu = \mu(\boldsymbol{z})$, где $\boldsymbol{z} = (z_1, \ldots, z_k)$ — набор переменных над $\mathbb{N}_0$. Множество $M^{\langle k \rangle}$ всех k-последовательностей над M является B-модулем относительно обычных операций над функциями.

Модуль $M^{\langle k \rangle}$ превращается в правый $B[X] = B[x_1, \ldots, x_k]$-модуль, если для полинома[1] $F = \sum\limits_{\boldsymbol{s}} f_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}}$ и последовательности $\mu \in M^{\langle k \rangle}$ положить

$$(\mu F)(\boldsymbol{z}) = \sum_{\boldsymbol{s}} \mu(\boldsymbol{z} + \boldsymbol{s}) f_{\boldsymbol{s}}. \tag{3.1}$$

Идеал $I \lhd B[X]$ называется *унитарным*, если существуют унитарные полиномы $F_1(x), \ldots, F_k(x) \in B[x]$ (от одной переменной), такие что

$$F_1(x_1), \ldots, F_k(x_k) \in I.$$

[1] Для $\boldsymbol{s} = (s_1, \ldots, s_k) \in \mathbb{N}_0^k$ пишем $\boldsymbol{x}^{\boldsymbol{s}} = x_1^{s_1} \ldots x_k^{s_k}$.

Рассмотрим аннулятор подмножества $\mathcal{M} \subseteq M^{\langle k\rangle}$ в кольце $B[X]$:

$$\rho_{B[X]}(\mathcal{M}) = \{F \in B[X] \mid \mathcal{M}F = 0\}.$$

Последовательность $\mu \in M^{\langle k\rangle}$ называется *k-линейной рекуррентной последовательностью* (*k-ЛРП*) над модулем M_B, если аннулятор $I = \rho_{B[X]}(\mu)$ — унитарный идеал. В этом случае полиномы (3.1) называются *элементарными характеристическими полиномами* k-линейной рекуррентной последовательности μ.

Предложение 3.1 ([17]). *Пусть кольцо B коммутативно, тогда имеют место следующие утверждения*:

1) *множество $\mathcal{L}M_B^{\langle k\rangle}$ всех k-ЛРП над M_B является подмодулем $M_{B[X]}^{\langle k\rangle}$*;
2) *для любого подмножества $\chi \subseteq B[X]$ семейство $L_M(\chi) = \lambda_{M^{\langle k\rangle}}(\chi) = \{\mu \in M^{\langle k\rangle} \mid \mu\chi = 0\}$ — подмодуль в $M_{B[X]}^{\langle k\rangle}$ и, более того, $L_M(\chi) \subseteq \mathcal{L}M_B^{\langle k\rangle}$ тогда и только тогда, когда $\chi B[X]$ — унитарный идеал в $B[X]$.*

Если I — унитарный идеал в $B[X]$, то множество $L_M(I)$ называется *k-ЛРП-семейством* над M_B.

Теорема 3.2 ([3, 8, 17, 21, 22]). *Пусть B — коммутативное артиново кольцо и Q_B — QF-модуль. Тогда для любого унитарного идеала $I \lhd B[X]$ ЛРП-семейство $L_Q(I)$ является QF-модулем над коммутативным артиновым кольцом $S = B[X]/I$ и эквивалентны следующие условия*:

1) $I = \rho_{B[X]}(\mu)$ *для некоторой рекурренты* $\mu \in \mathcal{L}Q_B^{\langle k\rangle}$;
2) $L_Q(I)$ — *циклический* $B[X]$*-модуль*;
3) S — *квазифробениусово кольцо*;
4) $(B[X]/\sqrt{I})_{\bar{B}} \cong [(I : \sqrt{I})/I]_{\bar{B}}$.

Пусть R, как и прежде, есть коммутативное артиново локальное кольцо главных идеалов. Кольцо R квазифробениусово, ввиду этого из теоремы 3.2 вытекает такое следствие.

Следствие 3.3. *Для унитарного идеала $I \lhd R[X]$ ЛРП-семейство $L_R(I)$ является циклическим $R[X]$-модулем, если и только если*

$$\dim_{\bar{R}}(R[X]/\sqrt{I}) = \dim_{\bar{R}}(I : \sqrt{I})/I. \tag{3.2}$$

Отметим, что критерий (3.2) для случая одной переменой ($k = 1$) был получен ранее в [19]. Теорема 3.2 представляет обобщение критерия из [19], причём её доказательство намного короче, так как использует хорошо известные свойства QF-колец.

Методы, основанные на стандартных базисах (см. разделы 1, 2), позволяют вычислить левую и правую части равенства (3.2), что даёт алгоритм, проверяющий, является ли ЛРП-семейство $L_R(I)$ циклическим $R[X]$-модулем. Чтобы сформулировать этот алгоритм, нам потребуется следующее утверждение.

Предложение 3.4. *Пусть I — идеал в $R[X]$ и $g_1, \ldots, g_m$ — семейство порождающих идеала $\sqrt{\bar{I}}$ в $\bar{R}[X]$. Тогда если полиномы $G_1, \ldots, G_m$ из $R[X]$ таковы, что*

$$\bar{G}_1 = g_1, \quad i \in \overline{1,m},$$

то идеал $\sqrt{I} \lhd R[X]$ порождается семейством полиномов

$$G_1, \ldots, G_m, \pi.$$

Доказательство. Так как $\pi \in \sqrt{I}$, то $\sqrt{I} = \sqrt{I + \pi R[X]}$ и, значит, для полинома $F \in R[X]$

$$F \in \sqrt{I} \iff \bar{F} \in \sqrt{\bar{I}},$$

откуда и следует наше утверждение. □

Предложение 3.4 показывает, что множество порождающих радикала $\sqrt{I}$ может быть эффективно построено исходя из системы порождающих идеала I с помощью соответствующего алгоритма для полей.

Предложения 2.4, 3.4, 3.3, алгоритмы из пункта 2.2 и алгоритм 1.46 позволяют сформулировать алгоритм 3.5.

Алгоритм 3.5. Проверка цикличности ЛРП-семейства.

INPUT: $\phi = \{F_1, \ldots, F_s\} \subset R[X]$ — система порождающих унитарного идеала $I \lhd R[X]$

OUTPUT: TRUE, если ЛРП-семейство $L_R(I)$ является циклическим $R[X]$-модулем, и **FALSE** в противном случае

С помощью алгоритмов для полей находим систему порождающих $g_1, \ldots, g_m$ идеала $\sqrt{\bar{I}}$

Строим полиномы $G_1, \ldots, G_m$, такие что $\bar{G}_i = g_i$, $i \in \overline{1,m}$

$\psi := \{G_1, \ldots, G_m, \pi\}$

Исходя из систем полиномов ϕ и ψ с помощью алгоритма из пункта 2.2 находим систему порождающих χ идеала $I : \sqrt{I}$

С помощью алгоритма 1.46 находим стандартные базисы ϕ', χ' и ψ' для идеалов $I = \phi R[X]$, $I : \sqrt{I} = \chi R[X]$ и $\sqrt{I} = \psi R[X]$ соответственно

IF $|[\pi, X] \setminus \mathrm{LM}(\psi')[\pi, X]| == |\mathrm{LM}(\chi')[\pi, X] \setminus \mathrm{LM}(\phi')[\pi, X]|$ **THEN**

RETURN TRUE

END IF

RETURN FALSE

Отметим, что для случая одной переменной ($k = 1$) алгоритм проверки цикличности ЛРП-семейства был построен ранее в [19].

3.2. Линейные регистры сдвига

В этом разделе решается сформулированная в [18] задача о построении критерия перестановочности сопутствующих эндоморфизмов в терминах полной системы $\mathcal{F}$-унитарных полиномов.

Произвольное конечное подмножество $\mathcal{F} \subset \mathbb{N}_0^k$ называется *полиэдром*. Полиэдр $\mathcal{F}$ называется *диаграммой Ферре*, если для любых $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}_0^k$

$$(\boldsymbol{i} \in \mathcal{F},\ \boldsymbol{j} \leqslant \boldsymbol{i}) \implies (\boldsymbol{j} \in \mathcal{F}),$$

где порядок $\leqslant$ на $\mathbb{N}_0^k$ определяется формулой (1.42).

Пусть B — кольцо и M_B — правый B-модуль. Для полиэдра $\mathcal{F}$ через $M^{\mathcal{F}}$ обозначим B-модуль всех функций $\delta\colon \mathcal{F} \to M$. Ясно, что модуль $M_B^{\mathcal{F}}$ изоморфен модулю $M_B^{|\mathcal{F}|}$. *Диаграммой значений* k-последовательности $\mu \in M^{\langle k \rangle}$ на полиэдре $\mathcal{F}$ называется ограничение $\mu|_{\mathcal{F}} \in M^{\mathcal{F}}$.

Пусть $\mathcal{F}$ — полиэдр и χ — система полиномов из $B[X] = B[x_1, \ldots, x_k]$. Если гомоморфизм абелевых групп

$$\sigma_{\mathcal{F}}\colon L_M(\chi) \to M^{\mathcal{F}}, \quad \sigma(\mu) = \mu|_{\mathcal{F}}, \tag{3.3}$$

является мономорфизмом, то говорят, что семейство $L_M(\chi)$ *рекурсивно конечно представлено* и $\mathcal{F}$ *— определяющий полиэдр* для χ и $L_M(\chi)$.

Определение 3.6. Пусть $\mathcal{F}$ — диаграмма Ферре и χ — система полиномов из $B[X]$. Пара $(\chi, \mathcal{F})$ называется *k-линейным регистром сдвига* или *$\mathcal{F}$-линейным регистром сдвига* над модулем M_B (кратко k-ЛРС или $\mathcal{F}$-ЛРС), если и только если гомоморфизм (3.3) является изоморфизмом. При этом ЛРП-семейство $L_M(\chi)$ называется множеством рекуррент, *порождённых* регистром сдвига $(\chi, \mathcal{F})$.

Пусть $\mathbf{1}_s$ — s-я строка единичной матрицы размера k. *Внутренностью, внутренней границей, внешней границей* диаграммы Ферре $\mathcal{F} \subset \mathbb{N}_0^k$ *в направлении* $\mathbf{1}_s$, $s \in \overline{1,k}$, назовём множества

$$\begin{aligned} \mathcal{F}_s &= \{\boldsymbol{r} \in \mathcal{F} \mid \boldsymbol{r} + \mathbf{1}_s \in \mathcal{F}\}, \\ \partial_s\mathcal{F} &= \mathcal{F} \setminus \mathcal{F}_s, \\ \Delta_s\mathcal{F} &= \partial_s\mathcal{F} + \mathbf{1}_s \end{aligned}$$

соответственно (см. рис. 1).

Объединение $\Delta\mathcal{F} = \bigcup\limits_{s=1}^{k} \Delta_s\mathcal{F}$ называется *внешней границей* диаграммы Ферре $\mathcal{F}$. Полином $H \in B[X]$ называется *$\mathcal{F}$-унитарным*, если для некоторого $\boldsymbol{r} \in \Delta\mathcal{F}$

$$H = \boldsymbol{x}^{\boldsymbol{r}} - \sum_{\boldsymbol{i} \in \mathcal{F}} h_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \tag{3.4}$$

(см. сноску на с. 58).

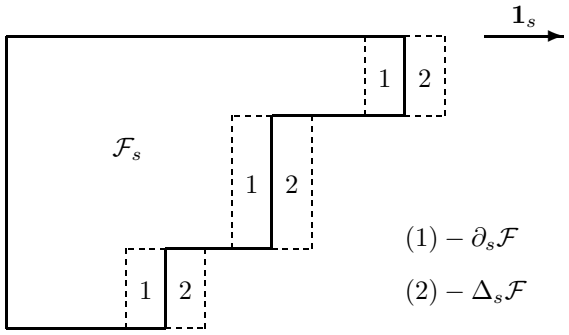

Рис. 1. Диаграмма Ферре

Множество $\Phi \subset B[X]$ из $|\Delta\mathcal{F}|$ полиномов называется *полной системой $\mathcal{F}$-унитарных полиномов*, если для каждого $\boldsymbol{r} \in \Delta\mathcal{F}$ эта система содержит единственный полином вида (3.4), то есть если Φ имеет вид

$$\Phi = \left\{ H_{\boldsymbol{r}} = \boldsymbol{x}^{\boldsymbol{r}} - \sum_{\boldsymbol{i}\in\mathcal{F}} h_{\boldsymbol{r},\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}} \;\middle|\; \boldsymbol{r} \in \Delta\mathcal{F} \right\}. \tag{3.5}$$

С каждой полной системой $\mathcal{F}$-унитарных полиномов (3.5) ассоциирован набор из k эндоморфизмов $\phi_1, \ldots, \phi_k$ модуля ${}_{B'}M$ ($B' = \mathrm{End}(M_B)$ — кольцо эндоморфизмов, действующих на M слева). Для любых $\delta \in M^{\mathcal{F}}$ и $\boldsymbol{j} \in \mathcal{F}$ полагаем

$$\phi_s(\delta)(\boldsymbol{j}) = \begin{cases} \delta(\boldsymbol{j} + \mathbf{1}_s), & \text{если } \boldsymbol{j} \in \mathcal{F}_s, \\ \sum\limits_{\boldsymbol{i}\in\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}}\delta(\boldsymbol{i}), & \text{если } \boldsymbol{j} \in \partial_s\mathcal{F}. \end{cases} \tag{3.6}$$

Эндоморфизмы $\phi_1, \ldots, \phi_k$ называются *сопутствующими эндоморфизмами* системы полиномов (3.5).

Кольцо $B'' = \mathrm{End}({}_{B'}M)$ называется *кольцом биэндоморфизмов* модуля M_B (см., например, [11]). Действие эндоморфизмов из B'' на элементы из M мы записываем как правые умножения, так что M превращается в бимодуль ${}_{B'}M_{B''}$. Для всякого $b \in B$ отображение

$$b^{(r)} \colon M \ni m \mapsto mb \in M$$

является элементом из B'', и соотношение

$$\beta \colon B \to B'', \quad \beta(b) = b^{(r)},$$

задаёт кольцевой гомоморфизм. Ядро $\mathrm{Ker}(\beta)$ совпадает с аннулятором $\rho_B(M)$, так что β является вложением, если и только если модуль M_B точен.

Теорема 3.7 ([18]). *Для любого $\mathcal{F}$-линейного регистра сдвига $(\chi, \mathcal{F})$ над M_B существует $\mathcal{F}$-линейный регистр сдвига $(\Phi, \mathcal{F})$ над $M_{B''}$, такой что Φ — полная система $\mathcal{F}$-унитарных полиномов из кольца $B''[X]$ и $L_M(\chi) = L_M(\Phi)$.*

$\mathcal{F}$-линейный регистр сдвига $(\chi, \mathcal{F})$ называется *каноническим $\mathcal{F}$-линейным регистром сдвига*, если χ — полная система $\mathcal{F}$-унитарных полиномов. Теорема 3.7 показывает, что множество рекуррент, порождённых любым регистром

сдвига, порождается некоторым каноническим регистром сдвига (возможно, над бóльшим кольцом). Ввиду этого представляет интерес задача отыскания условий на систему $\mathcal{F}$-унитарных полиномов Φ, дающих критерий того, что $(\Phi, \mathcal{F})$ есть k-линейный регистр сдвига.

Теорема 3.8 ([18]). *Пусть $\mathcal{F}$ — диаграмма Ферре и Φ — полная система $\mathcal{F}$-унитарных полиномов из $B[X]$ вида* (3.5). *Тогда пара $(\Phi, \mathcal{F})$ является k-линейным регистром сдвига, если и только если сопутствующие эндоморфизмы $\phi_1, \ldots, \phi_k$ попарно перестановочны.*

Мы дадим критерий перестановочности сопутствующих эндоморфизмов, апеллирующий к коэффициентам полиномов из Φ, решив тем самым одну из поставленных в [18] задач.

Теорема 3.9. *Пусть $\mathcal{F}$ — диаграмма Ферре, Φ — полная система $\mathcal{F}$-унитарных полиномов из $B[X]$ вида* (3.5) *и $\rho = \rho_B(M)$ — аннулятор модуля M в B. Тогда сопутствующие эндоморфизмы $\phi_1, \ldots, \phi_k$ попарно перестановочны, если и только если для любых $s, t \in \overline{1,k}$, $s \neq t$, выполняются следующие условия: для $\boldsymbol{j} \in \partial_s\mathcal{F} \cap \mathcal{F}_t$*

$$H_{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_s} \overset{\rho}{\equiv} H_{\boldsymbol{j}+\mathbf{1}_s} x_t + \sum_{\boldsymbol{k}\in\partial_t\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}} H_{\boldsymbol{k}+\mathbf{1}_t} \tag{3.7}$$

и для $\boldsymbol{j} \in \partial_s\mathcal{F} \cap \partial_t\mathcal{F}$

$$H_{\boldsymbol{j}+\mathbf{1}_s} x_t + \sum_{\boldsymbol{k}\in\partial_t\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}} H_{\boldsymbol{k}+\mathbf{1}_t} \overset{\rho}{\equiv} H_{\boldsymbol{j}+\mathbf{1}_t} x_s + \sum_{\boldsymbol{k}\in\partial_s\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_t,\boldsymbol{k}} H_{\boldsymbol{k}+\mathbf{1}_s}. \tag{3.8}$$

Доказательство. Для любых $\alpha \in M$ и $\boldsymbol{i} \in \mathcal{F}$ определим функцию $\alpha_{\boldsymbol{i}} \in M^{\mathcal{F}}$, а именно для любого $\boldsymbol{j} \in \mathcal{F}$ положим

$$\alpha_{\boldsymbol{i}}(\boldsymbol{j}) = \begin{cases} \alpha, & \text{если } \boldsymbol{j} = \boldsymbol{i}, \\ 0, & \text{если } \boldsymbol{j} \neq \boldsymbol{i}. \end{cases}$$

Ясно, что эндоморфизмы ϕ_s и ϕ_t коммутируют в том и только том случае, когда для любых $\alpha \in M$ и $\boldsymbol{i}, \boldsymbol{j} \in \mathcal{F}$

$$(\phi_s\phi_t(\alpha_{\boldsymbol{i}}))(\boldsymbol{j}) = (\phi_t\phi_s(\alpha_{\boldsymbol{i}}))(\boldsymbol{j}). \tag{3.9}$$

Распишем подробно левую часть равенства (3.9):

$$(\phi_s\phi_t(\alpha_{\boldsymbol{i}}))(\boldsymbol{j}) = [\phi_s(\phi_t\alpha_{\boldsymbol{i}})](\boldsymbol{j}) = \begin{cases} (\phi_t\alpha_{\boldsymbol{i}})(\boldsymbol{j}+\mathbf{1}_s) & \text{при } \boldsymbol{j} \in \mathcal{F}_s, \\ \sum\limits_{\boldsymbol{k}\in\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}(\phi_t\alpha_{\boldsymbol{i}})(\boldsymbol{k}) & \text{при } \boldsymbol{j} \in \partial_s\mathcal{F}. \end{cases}$$

Используя выражение вида (3.6) для $\phi_t\alpha_{\boldsymbol{i}}$, находим, что элемент $(\phi_s\phi_t(\alpha_{\boldsymbol{i}}))(\boldsymbol{j})$ равен

$$\begin{cases} \alpha_{\boldsymbol{i}}(\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t) & \text{при } \boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t\in\mathcal{F},\\ \alpha\cdot h_{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t,\boldsymbol{i}} & \text{при } \boldsymbol{j}\in\mathcal{F}_s,\ \boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t\notin\mathcal{F},\\ \alpha\cdot\Big(h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}-\mathbf{1}_t}+\sum\limits_{\boldsymbol{k}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\Big) & \text{при } \boldsymbol{j}\in\partial_s\mathcal{F},\ \boldsymbol{i}\geqslant\mathbf{1}_t,\\ \alpha\cdot\sum\limits_{\boldsymbol{k}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}} & \text{при } \boldsymbol{j}\in\partial_s\mathcal{F},\ \boldsymbol{i}\not\geqslant\mathbf{1}_t. \end{cases}$$

Заметим, что в приведённом выше представлении третья и четвёртая строчки могут быть объединены в одну, если дополнительно определить, что $h_{\boldsymbol{r},\boldsymbol{i}}=0$ при наличии отрицательных координат в векторе $\boldsymbol{i}\in\mathbb{Z}_0^k$. В дальнейшем мы придерживаемся этого соглашения.

В соответствии с равенством

$$\mathcal{F}=(\mathcal{F}_s\cap\mathcal{F}_t)\sqcup(\partial_s\mathcal{F}\cap\mathcal{F}_t)\sqcup(\mathcal{F}_s\cap\partial_t\mathcal{F})\sqcup(\partial_s\mathcal{F}\cap\partial_t\mathcal{F})$$

рассмотрим четыре логически возможных случая.

1. $\boldsymbol{j}\in\mathcal{F}_s\cap\mathcal{F}_t$. Если $\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t\in\mathcal{F}$, то левая и правая части (3.9) равны $\alpha_{\boldsymbol{i}}(\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t)$. Если $\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t\notin\mathcal{F}$, то обе части (3.9) равны $\alpha\cdot h_{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t,\boldsymbol{i}}$. Значит, при $\boldsymbol{j}\in\mathcal{F}_s\cap\mathcal{F}_t$ равенство (3.9) выполняется всегда.

2. $\boldsymbol{j}\in\partial_s\mathcal{F}\cap\mathcal{F}_t$. В этом случае $\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t\notin\mathcal{F}$ и, значит, равенство (3.9) равносильно соотношению

$$\alpha\cdot\Big(h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}-\mathbf{1}_t}+\sum_{\boldsymbol{k}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\Big)=\alpha\cdot h_{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t,\boldsymbol{i}}.$$

3. $\boldsymbol{j}\in\mathcal{F}_s\cap\partial_t\mathcal{F}$. Этот случай аналогичен предыдущему.

4. $\boldsymbol{j}\in\partial_s\mathcal{F}\cap\partial_t\mathcal{F}$. В этом случае равенство (3.9) эквивалентно соотношению

$$\alpha\cdot\Big(h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}-\mathbf{1}_t}+\sum_{\boldsymbol{k}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\Big)=\alpha\cdot\Big(h_{\boldsymbol{j}+\mathbf{1}_t,\boldsymbol{i}-\mathbf{1}_s}+\sum_{\boldsymbol{k}\in\partial_s\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_t,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_s,\boldsymbol{i}}\Big).$$

Домножая левую и правую части равенства из пункта 2 на $\boldsymbol{x}^{\boldsymbol{i}}$ и суммируя по $\boldsymbol{i}\in\mathcal{F}$, получим соотношение

$$\sum_{\boldsymbol{i}\in\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}-\mathbf{1}_t}\boldsymbol{x}^{\boldsymbol{i}}+\sum_{\boldsymbol{i}\in\mathcal{F}}\Big(\sum_{\boldsymbol{k}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\Big)\boldsymbol{x}^{\boldsymbol{i}}\overset{\rho}{\equiv}\sum_{\boldsymbol{i}\in\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t,\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}\qquad(3.10)$$

(ввиду произвольности $\alpha\in M$ в соотношениях из пунктов 2—4 можно удалить α, заменив знак равенства на $\overset{\rho}{\equiv}$). Имеем

$$\sum_{\boldsymbol{i}\in\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}-\mathbf{1}_t}\boldsymbol{x}^{\boldsymbol{i}}=\Big(\sum_{\boldsymbol{i}\in\mathcal{F}_t}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}\Big)x_t=$$

$$=\boldsymbol{x}^{\boldsymbol{j}+\mathbf{1}_s+\mathbf{1}_t}-H_{\boldsymbol{j}+\mathbf{1}_s}x_t-\sum_{\boldsymbol{i}\in\partial_t\mathcal{F}}h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}+\mathbf{1}_t}$$

и

$$\sum_{\boldsymbol{i}\in\mathcal{F}}\Big(\sum_{\boldsymbol{k}\in\partial_t\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\Big)\boldsymbol{x}^{\boldsymbol{i}} = \sum_{\boldsymbol{k}\in\partial_t\mathcal{F}}\Big(h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}\sum_{\boldsymbol{i}\in\mathcal{F}} h_{\boldsymbol{k}+\mathbf{1}_t,\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}\Big) = \\ = \sum_{\boldsymbol{k}\in\partial_t\mathcal{F}} h_{\boldsymbol{j}+\mathbf{1}_s,\boldsymbol{k}}(\boldsymbol{x}^{\boldsymbol{k}+\mathbf{1}_t} - H_{\boldsymbol{k}+\mathbf{1}_t}),$$

откуда вытекает, что условие (3.10) равносильно соотношению (3.7). Рассуждая аналогично, находим, что условие из пункта 4 эквивалентно соотношению (3.8). □

Пусть S — произвольное кольцо с единицей и M_S, N_S — правые S-модули. Известно (см., например, [4, 11]), что множество $\mathrm{Hom}_S(M,N)$ превращается в абелеву группу, если для любых $\alpha,\beta\in\mathrm{Hom}_S(M,N)$ положить

$$(\alpha+\beta)(m) = \alpha(m)+\beta(m), \quad m\in M.$$

Более того, если теперь T — ещё одно кольцо с единицей и на M задана структура T-S-бимодуля ${}_TM_S$, то $\mathrm{Hom}_S(M,N)$ с помощью определения

$$(\alpha t)(m) = \alpha(tm), \quad \alpha\in\mathrm{Hom}_S(M,N), \quad m\in M, \quad t\in T,$$

превращается в правый T-модуль.

Пусть теперь B — кольцо с единицей и M_B — правый B-модуль. Кольцо полиномов $B[X]$ можно рассматривать как $B[X]$-B-бимодуль, так что в соответствии со сказанным выше множество $\mathrm{Hom}_B(B[X],M_B)$ естественным образом наделяется структурой правого $B[X]$-модуля. Аналогично, для любого двустороннего идеала I $\mathrm{Hom}_B(B[X]/I,M_B)$ можно рассматривать как правый $B[X]$-модуль. Более того, имеет место следующее утверждение.

Предложение 3.10. *Пусть B — кольцо с единицей и M_B — правый B-модуль, тогда справедливы следующие утверждения.*

1. *Отображение*
$$\Lambda\colon \mathrm{Hom}_B(B[X],M_B)\ni\phi\mapsto\mu\in M^{\langle k\rangle},$$
задаваемое равенством
$$\mu(\boldsymbol{z}) = \phi(\boldsymbol{x}^{\boldsymbol{z}}), \quad \boldsymbol{z}\in\mathbb{N}_0^k,$$
является изоморфизмом правых $B[X]$-модулей.
2. *Для любого правого (двустороннего) идеала I из $B[X]$ отображение*
$$\Lambda_I\colon \mathrm{Hom}_B(B[X]/I,M_B)\ni\phi\mapsto\mu\in L_M(I), \tag{3.11}$$
задаваемое равенством
$$\mu(\boldsymbol{z}) = \phi(\boldsymbol{x}^{\boldsymbol{z}}+I), \quad \boldsymbol{z}\in\mathbb{N}_0^k,$$
является изоморфизмом абелевых групп (правых $B[X]$-модулей).

Доказательство. То, что отображение Λ является изоморфизмом абелевых групп, следует из того, что $B[X]$ является свободным правым B-модулем с базисом $[X] = \{\boldsymbol{x}^{\boldsymbol{z}} \mid \boldsymbol{z} \in \mathbb{N}_0^k\}$. Пусть $F = \sum\limits_{\boldsymbol{s}} f_{\boldsymbol{s}}\boldsymbol{x}^{\boldsymbol{s}}$ — полином из $B[X]$ и $\phi \in \mathrm{Hom}_B(B[X], M_B)$, тогда

$$[\Lambda(\phi F)](\boldsymbol{z}) = (\phi F)(\boldsymbol{x}^{\boldsymbol{z}}) = \phi(F\boldsymbol{x}^{\boldsymbol{z}}) = \phi\Big(\sum_{\boldsymbol{s}} f_{\boldsymbol{s}}\boldsymbol{x}^{\boldsymbol{s}+\boldsymbol{z}}\Big) =$$

$$= \sum_{\boldsymbol{s}} \phi(\boldsymbol{x}^{\boldsymbol{s}+\boldsymbol{z}})f_{\boldsymbol{s}} = \sum_{\boldsymbol{s}} [\Lambda(\phi)](\boldsymbol{s}+\boldsymbol{z})f_{\boldsymbol{s}} = [\Lambda(\phi)F](\boldsymbol{z}).$$

Значит, Λ является $B[X]$-изоморфизмом.

Утверждение пункта 2 следует из 1 и из следующего легко проверяемого соотношения:

$$\Lambda(\phi) \in L_M(I) \iff I \subseteq \mathrm{Ker}\,\phi$$

для любого $\phi \in \mathrm{Hom}_B(B[X], M_B)$. □

Напомним (см. также [4,11]), что модуль C_B называется кообразующим в категории правых B-модулей $\mathcal{M}_B$, если для любого модуля M_B имеет место равенство

$$\mathrm{Ker}(M, C) = \bigcap_{\phi \in \mathrm{Hom}_B(M,C)} \mathrm{Ker}\,\phi = 0.$$

Лемма 3.11. *Пусть N_B — модуль и $X = (x_\alpha \mid \alpha \in A)$ — семейство элементов из N. Пусть C_B — кообразующий в $\mathcal{M}_B$. Тогда N_B является свободным модулем с базисом X в том и только том случае, когда гомоморфизм абелевых групп*

$$\Psi\colon\ \mathrm{Hom}_B(N, C) \to C^A,$$

определяемый соотношением

$$[\Psi(\phi)](\alpha) = \phi(x_\alpha),$$

является изоморфизмом.

Доказательство. Если X — базис N_B, то Ψ является изоморфизмом по определению свободного модуля.

Обратно, пусть Ψ — изоморфизм. Допустим, что существует элемент $a \in F$, не принадлежащий подмодулю K модуля N_B, порождённому X. Тогда элемент $a + K \in N/K$ не равен 0 и, значит, поскольку C_B — кообразующий, найдётся такой гомоморфизм $\psi\colon N/K \to C$, что $\psi(a + K) \neq 0$. Пусть $\nu\colon N \to N/K$ — естественный эпиморфизм, тогда гомоморфизм $\phi = \psi\nu \in \mathrm{Hom}_B(N, C)$ таков, что $\phi(K) = 0$ и $\phi(a) \neq 0$. Имеем $\Psi(\phi) = 0$ и, следовательно, в силу предположения, $\psi = 0$ — пришли к противоречию. Значит, $N = K$.

Осталось доказать, что X — свободная система. Допустим, напротив, что существуют набор $b_1, \ldots, b_n$, $n \geqslant 1$, ненулевых элементов из B и попарно различные индексы $\alpha_1, \ldots, \alpha_n \in A$, такие что

$$x_{\alpha_1}b_1 + \ldots + x_{\alpha_1}b_1 = 0. \tag{3.12}$$

Рассмотрим какой-нибудь свободный B-модуль F (например, можно положить $F = B^n$) с базисом $e_1, \ldots, e_n$. Элемент $y = e_1 b_1 + \ldots + e_n b_n \in F$ не равен 0, и, значит, найдётся гомоморфизм $\chi\colon F \to C$, такой что $\chi(y) \neq 0$. Положим $c_i = \chi(e_i)$ для $i \in \overline{1,n}$, тогда

$$c_1 b_1 + \ldots + c_n b_n \neq 0. \tag{3.13}$$

По предположению найдётся такой гомоморфизм $\phi\colon N \to C$, что $\phi(x_{\alpha_i}) = c_i$, $i \in \overline{1,n}$, что невозможно ввиду (3.12) и (3.13). □

Теорема 3.12. *Пусть B — произвольное кольцо, I — правый идеал в $B[X]$, $\mathcal{F} \subseteq \mathbb{N}_0^k$ — диаграмма Ферре и C_B — кообразующий в $\mathcal{M}_B$. Тогда эквивалентны следующие условия*:

1) *$B[X]/I$ — свободный правый B-модуль с базисом $(\boldsymbol{x}^{\boldsymbol{z}} + I \mid \boldsymbol{z} \in \mathcal{F})$;*
2) *пара $(I, \mathcal{F})$ является регистром сдвига над любым модулем из $\mathcal{M}_B$;*
3) *пара $(I, \mathcal{F})$ является регистром сдвига над C_B.*

Доказательство. Докажем импликацию 1) $\Longrightarrow$ 2). Пусть M_B — произвольный правый B-модуль. Рассмотрим гомоморфизм абелевых групп $\Psi_M = \sigma_{\mathcal{F}} \Lambda_I$ (см. (3.3) и (3.11))

$$\Psi_M\colon \operatorname{Hom}_B(B[X]/I, M_B) \to M^{\mathcal{F}}.$$

Отображение Ψ_M ставит в соответствие гомоморфизму ϕ набор его значений на $\{\boldsymbol{x}^{\boldsymbol{z}} + I \mid \boldsymbol{z} \in \mathcal{F}\}$. Следовательно, ввиду 1) Ψ является изоморфизмом. Согласно предложению 3.10 Λ_I — изоморфизм, и, следовательно, $\sigma_{\mathcal{F}}$ — изоморфизм.

Импликация 2) $\Longrightarrow$ 3) очевидна.

Убедимся, что справедлива импликация 3) $\Longrightarrow$ 1). Если $(I, \mathcal{F})$ — регистр сдвига над C_B, то σ_F — изоморфизм, и, следовательно, Φ_C также является изоморфизмом. Утверждение следует теперь из леммы 3.11. □

Отметим, что эквивалентность (1) $\Longleftrightarrow$ (3) для случая, когда B — коммутативное артиново кольцо, C_B — квазифробениусов модуль и I — унитарный идеал, была получена ранее в [9].

Лемма 3.13 ([18]). *Пусть кольцо B нётерово справа, тогда правый идеал I из $B[X]$ унитарен в том и только том случае, когда $B[X]/I$ является конечно порождённым правым B-модулем.*

Из теоремы 3.12 и леммы 3.13 легко выводится такое следствие.

Следствие 3.14. *Пусть выполняются условия теоремы* 3.12 *и кольцо B нётерово справа. Тогда если пара $(I, \mathcal{F})$ является регистром сдвига над C_B, то I — унитарный идеал.*

3.3. Цилиндрические идеалы и поднятия

Теорема 3.15 ([2]). *Для произвольного идеала $I \lhd R[X]$ эквивалентны следующие условия*:

1) *I выделяется прямым слагаемым в $R[X]_R$*;
2) *I является свободным R-модулем*;
3) *$R[X]/I$ является свободным R-модулем*;
4) $\pi I = I \cap \pi R[X]$;
5) *$I = 0$ или I обладает π-однородным стандартным базисом нормы* 0.

Идеалы, для которых выполняются эквивалентные условия теоремы 3.15, были названы в [2] *цилиндрическими*.

Отметим, что в работе [9] для случая унитарного идеала I было доказано, что каноническая система образующих идеала является π-однородной системой нормы 0 в том и только том случае, когда $R[X]/I$ — свободный R-модуль [9, теорема 4.15], то есть фактически была доказана эквивалентность 3) $\iff$ 5) из теоремы 3.15.

Пусть $I \lhd R[X]$ — унитарный идеал и $\chi \subseteq I$ — редуцированная π-однородная система полиномов нормы 0, такая что $\bar{\chi}$ — редуцированный базис Грёбнера идеала $\bar{I}$, то есть в определениях работы [9] χ — круллева система. В [9] было доказано, что из свободности R-модуля $R[X]/I$ следует, что $\mathfrak{G}_\chi$ — схема симплификации с канонизацией. Там же был поставлен вопрос об обращении этой импликации. Мы утверждаем, что ответ на этот вопрос положителен. Действительно, χ — стандартный базис идеала I (теорема 1.44), являющийся π-однородной системой нормы 0. Следовательно, по теореме 3.15 $R[X]/I$ — свободный R-модуль.

Определение 3.16. Будем говорить, что базис Грёбнера $\psi \subseteq \bar{R}[X]$ *поднимается* (*в* $R[X]$), если существует π-однородная система $\chi \subseteq R[X]$ нормы 0, являющаяся стандартным базисом, такая что $\bar{\chi} = \psi$ и $\bar{G}_1 \neq \bar{G}_2$ для различных $G_1, G_2 \in \chi$. При этом систему χ будем называть *поднятием* системы ψ.

Теорема 3.17 ([2]). *Для любого ненулевого идеала $J \lhd \bar{R}[X]$ эквивалентны следующие условия*:

1) *любой базис Грёбнера идеала J поднимается*;
2) *существует базис Грёбнера идеала J, который поднимается*;
3) *существует цилиндрический идеал $I \lhd R[X]$, такой что $\bar{I} = J$.*

Для любого унитарного идеала $I \lhd R[X]$ существует диаграмма Ферре $\mathcal{F} \subseteq \mathbb{N}_0^k$, такая что

$$[X] \setminus \mathrm{LM}(I) = \{\boldsymbol{x}^{\boldsymbol{i}} \mid \boldsymbol{i} \in \mathcal{F}\}.$$

Говорят, что $\mathcal{F} = \mathcal{F}(I)$ — *опорная диаграмма Ферре* идеала I.

Следующая теорема устанавливает связь между k-линейными регистрами сдвига над R_R и цилиндрическими идеалами.

Теорема 3.18 ([9, 6.6]). *Пусть $I \lhd R[X]$ — унитарный идеал с опорной диаграммой Ферре $\mathcal{F}$. Тогда пара $(I, \mathcal{F})$ является k-линейным регистром сдвига над R_R, если и только если идеал I цилиндрический.*

Пусть

$$L_\alpha(y_{\boldsymbol{r},\boldsymbol{i}}) = 0, \quad \alpha \in \overline{1,m}, - \tag{3.14}$$

система уравнений относительно переменных $y_{\boldsymbol{r},\boldsymbol{i}}$, $\boldsymbol{r} \in \Delta\mathcal{F}$, $\boldsymbol{i} \in \mathcal{F}$, такая что условия (3.7) и (3.8) выполняются в том и только том случае, когда набор коэффициентов $h_{\boldsymbol{r},\boldsymbol{i}}$, $\boldsymbol{r} \in \Delta\mathcal{F}$, $\boldsymbol{i} \in \mathcal{F}$, является её корнем. Такую систему уравнений можно получить, записав соотношения (3.7) и (3.8) как условия на коэффициенты.

Пусть J — унитарный идеал в $\bar{R}[X]$ с опорной диаграммой Ферре $\mathcal{F}$ и ψ — редуцированный базис Грёбнера для J. Рассмотрим систему полиномов

$$\phi = \{f_{\boldsymbol{r}} = \boldsymbol{x}^{\boldsymbol{r}} - \mathrm{Can}_{\mathfrak{G}_\psi}(\boldsymbol{x}^{\boldsymbol{r}}) \mid \boldsymbol{r} \in \Delta\mathcal{F}\}.$$

Ясно, что $\psi \subseteq \phi$ и ϕ — полная система $\mathcal{F}$-унитарных полиномов из $\bar{R}[X]$.

Согласно теореме 3.18 пара $(\phi, \mathcal{F})$ является k-линейным регистром сдвига над $\bar{R}_{\bar{R}}$, и, значит, набор коэффициентов

$$(f_{\boldsymbol{r},\boldsymbol{i}} \mid \boldsymbol{r} \in \Delta\mathcal{F},\ \boldsymbol{i} \in \mathcal{F}) \tag{3.15}$$

полиномов из ϕ является корнем (3.14).

Предложение 3.19. *Во введённых выше обозначениях базис Грёбнера ψ идеала J поднимается тогда и только тогда, когда существует вектор*

$$(h_{\boldsymbol{r},\boldsymbol{i}} \in R \mid \boldsymbol{r} \in \Delta\mathcal{F},\ \boldsymbol{i} \in \mathcal{F}), \tag{3.16}$$

являющийся корнем (3.14)*, такой что*

$$\bar{h}_{\boldsymbol{r},\boldsymbol{i}} = f_{\boldsymbol{r},\boldsymbol{i}}, \quad \boldsymbol{r} \in \Delta\mathcal{F}, \quad \boldsymbol{i} \in \mathcal{F}.$$

Иными словами, базис Грёбнера ψ поднимается тогда и только тогда, когда поднимается корень (3.15) *системы уравнений* (3.14).

Доказательство. Пусть базис Грёбнера ψ поднимается, тогда согласно определению существует π-однородная система $\chi \subseteq R[X]$ нормы 0, являющаяся стандартным базисом, такая что $\bar{\chi} = \psi$ и $|\chi| = |\psi|$. Применяя алгоритм 1.55 к χ, найдём $\mathfrak{G}$-редуцированный стандартный базис χ' для идеала $\chi R[X]$. Легко видеть, что $\bar{\chi}' = \bar{\chi}$. По теореме 3.18 пара $(\chi', \mathcal{F})$ образует k-линейный регистр сдвига, и, следовательно, согласно теореме 3.9 вектор, образованный коэффициентами полиномов из χ', будет поднятием корня (3.15) системы уравнений (3.14).

Обратно, пусть корень (3.15) системы уравнений (3.14) поднимается до корня (3.16). Согласно теореме 3.9 полная система $\mathcal{F}$-унитарных полиномов

$$\Phi = \left\{ H_{\boldsymbol{r}} = \boldsymbol{x}^{\boldsymbol{r}} - \sum_{\boldsymbol{i} \in \mathcal{F}} h_{\boldsymbol{r},\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \;\middle|\; \boldsymbol{r} \in \Delta\mathcal{F} \right\},$$

построенная по вектору (3.16), вместе с $\mathcal{F}$ образует k-линейный регистр сдвига. Значит, по теореме 3.18 идеал $I = \Phi R[X]$ цилиндрический. Наше утверждение следует теперь из теоремы 3.17 и равенства $\bar{I} = \bar{\Phi}\bar{R}[X] = \psi\bar{R}[X] = J$. □

В [10] для случая колец Галуа построен алгоритм подъёма корней для произвольных систем полиномиальных уравнений. Применяя этот алгоритм к системе (3.14) и корню (3.15), получаем эффективную процедуру проверки существования, и нахождения в случае существования, поднятия базиса Грёбнера ψ.

Автор глубоко благодарен Александру Александровичу Нечаеву и Александру Васильевичу Михалёву за постановку задач, детальное обсуждение результатов работы и многочисленные важные замечания.

Литература

[1] Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: Мир, 1972.

[2] Горбатов Е. В. Стандартный базис полиномиального идеала над коммутативным артиновым цепным кольцом // Дискрет. мат. — 2004. — Т. 16, № 1. — С. 52—78.

[3] Горбатов Е. В., Нечаев А. А. Критерий цикличности семейства полилинейных рекуррент над QF-модулем // Успехи мат. наук. — 2001. — Т. 56, № 4.

[4] Каш Ф. Модули и кольца. — М.: Мир, 1981.

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

[6] Латышев В. Н. Комбинаторная теория колец, стандартные базисы. — М.: Изд-во Моск. ун-та, 1988.

[7] Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами // Дискрет. мат. — 1991. — Т. 3, № 4. — С. 105—127.

[8] Нечаев А. А. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам // Фундам. и прикл. мат. — 1995. — Т. 1, № 1. — С. 229—254.

[9] Нечаев А. А., Михайлов Д. А. Каноническая система образующих унитарного полиномиального идеала над коммутативным артиновым цепным кольцом // Дискрет. мат. — 2001. — Т. 13, № 4. — С. 3—42.

[10] Нечаев А. А., Михайлов Д. А. Решение системы полиномиальных уравнений над кольцом Галуа—Эйзенштейна с помощью канонической системы образующих полиномиального идеала // Дискрет. мат. — 2004. — Т. 16, № 4. — С. 21—51.

[11] Фейс К. Алгебра: кольца, модули, категории. Т. 2. — М.: Мир, 1979.

[12] Adams W., Loustaunau P. An Introduction to Gröbner bases. — Providence: American Mathematical Society, 1994. — Graduate Studies in Mathematics. Vol. 3.

[13] Apel J. Computational ideal theory in finitely generated extension rings // J. Theoretical Computer Science. — 2000. — Vol. 244. — P. 1—33.

[14] Byrne E., Fitzpatrick P. Gröbner bases over Galois rings with an application to decoding alternant codes // J. Symbolic Comput. — 2001. — Vol. 31. — P. 565—584.

[15] Kronecker L. Vorlesungen über Zahlentheorie. Bd. 1. — Leipzig: Teubner, 1901.

[16] Krull W. Algebraische Theorie der Ringe, II // Math. Ann. — 1923. — Bd. 91. — P. 1—46.

[17] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. — 1995. — Vol. 76, no. 6. — P. 2793—2915.

[18] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N. Linear and polylinear recurring sequences over Abelian groups and modules // J. Math. Sci. — 2000. — Vol. 102, no. 6. — P. 4598—4626.

[19] Lu P. A criterion for annihilating ideals of linear recurring sequences over Galois rings. — AAECC-417.

[20] Mora T. Seven Variations on Standard Bases. — Preprint. Univ. de Genova, Dip. di Mathematica. No. 45. — 1986.

[21] Nechaev A. A. Linear recurring sequences over quasi-Frobenius modules // Russian Math. Surveys. — 1993. — Vol. 48, no. 3.

[22] Nechaev A. A. Polylinear recurring sequences over modules and quasi-Frobenius modules // Proc. First Int. Tainan–Moscow Algebra Workshop, 1994. — Berlin, New York: Walter de Gruyter, 1996. — P. 283—298.

[23] Norton G. H., Salagean A. Strong Gröbner bases and cyclic codes over a finite-chain ring // Proceedings of the International Workshop on Coding and Cryptography. — Paris, 2001. — P. 8—12.

[24] Robbiano L. On the theory of graded structures // J. Symbolic Comput. — 1986. — Vol. 2. — P. 139—170.