Мультипликативные порядки на одночленах*

Е. В. ГОРБАТОВ
Московский государственный университет им. М. В. Ломоносова

УДК 512.714+512.536

Ключевые слова: коммутативное кольцо, алгебра полиномов, порядок на одночленах, старший член, мультипликативный порядок.

Аннотация

Пусть R — коммутативное кольцо с единицей. Всякий порядок на одночленах из кольца $R[x_1, \ldots, x_k]$ естественным образом индуцирует понятие старшего члена полинома. Порядок называется мультипликативным, если произведение старших членов равно старшему члену произведения. В работе приведена конструкция, позволяющая строить мультипликативные порядки. Получен ряд свойств, характеризующих кольца, для которых такие порядки существуют. Приведены достаточные условия наличия таких порядков.

Abstract

E. V. Gorbatov, Multiplicative orders on terms, Fundamentalnaya i prikladnaya matematika, vol. 13 (2007), no. 1, pp. 101—107.

Let R be a commutative ring with identity. Any order on terms of the polynomial algebra $R[x_1, \ldots, x_k]$ induces in a natural way the notion of a leading term. An order on terms is called multiplicative if and only if the leading term of a product equals the product of leading terms. In this paper, we present a procedure for the construction of multiplicative orders. We obtain some characterizations of rings for which such orders exist. We give conditions sufficient for the existence of such orders.

Введение

Для решения многих прикладных задач современной алгебры (например, связанных с полилинейными рекуррентными последовательностями и линейными кодами над конечными кольцами и модулями) можно использовать технику стандартных базисов (базисов Грёбнера—Ширшова) полиномиальных идеалов, общая теория которых в настоящее время хорошо развита (см. [3, 7]). Однако попытки использовать стандартные базисы, которые строятся по известным общим алгоритмам, показали, что эти базисы малоэффективны.

*Работа выполнена при поддержке грантов РФФИ 02-01-00218 и НШ-1910.2003.1.

Фундаментальная и прикладная математика, 2007, том 13, № 1, с. 101—107.

Алгоритмы построения стандартных базисов идеалов кольца $R[X]$ основаны на некотором упорядочении одночленов $rx_1^{i_1}\dots x_k^{i_k}$ 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. В [4] в случае, когда R — коммутативное конечно-цепное кольцо, был предложен порядок на одночленах, учитывающий эту специфику: место идеала rR в конечной цепи идеалов кольца R. Дальнейшие исследования (см. [1,2,5,6]) выявили, что стандартные базисы, основанные на таком упорядочении одночленов, позволяют решить многие из поставленных задач.

Важной особенностью порядка из [4] является его *мультипликативность*. При определении старшего члена полинома согласно этому порядку выполняется следующее свойство: старший член произведения равен произведению старших членов. Такой порядок существует не для всякого кольца R.

Вопрос описания класса колец, для которых можно определить мультипликативный порядок на одночленах, остаётся открытым. В работе приводятся некоторые достаточные и некоторые необходимые условия существования мультипликативных порядков. Приводятся примеры, уточняющие эти условия.

Мультипликативные порядки

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* называется подполугруппа

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

полугруппы $(R[X],\cdot)$.

Порядок (т. е. транзитивное, рефлексивное, антисимметричное отношение) $\preccurlyeq$ на $[R,X]$ называется *разделяющим мономы* [1], 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 $\preccurlyeq$ заданы $\succcurlyeq$, $\prec$, $\succ$, при этом, например, $a\prec b \iff (a\preccurlyeq b)\ \&\ (a\neq b)$.)

При заданном разделяющим мономы порядке $\preccurlyeq$ на $[R,X]$ всякий ненулевой полином $F\in R[X]$ можно представить в виде

$$F=a_1u_1+a_2u_2+\dots+a_nu_n, \tag{1}$$

где $a_i\in R\setminus 0$, мономы u_i попарно различны и $a_1u_1\succ a_2u_2\succ\dots\succ a_nu_n$. *Ведущим членом* полинома F *относительно порядка* $\preccurlyeq$ называется

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

Также полагают, что $\mathrm{lt}_{\preccurlyeq}(0)=0$.

Имеет место следующее утверждение.

Предложение 1 ([1]). *Пусть* $\preccurlyeq$ *— разделяющий мономы порядок на* $[R, X]$. *Тогда следующие условия эквивалентны*:

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

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

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

$$\left.\begin{array}{l} au \prec bv \\ u \neq v \\ ac \neq 0,\ bc \neq 0 \end{array}\right| \implies acuw \prec bcvw \tag{2}$$

и

$$\left.\begin{array}{l} au \prec bv,\ bc = 0 \\ u \neq v \\ a \neq 0,\ b \neq 0 \end{array}\right| \implies ac = 0. \tag{3}$$

Разделяющий мономы порядок $\preccurlyeq$ на $[R, X]$, удовлетворяющий равносильным условиям а) и б) из предложения 1, называется *мультипликативным* [1].

Будем говорить, что коммутативное кольцо с единицей R *допускает мультипликативный порядок* (*на одночленах*), если на полугруппе $[R, X]$ существует мультипликативный порядок.

Представляет интерес описание класса колец R, допускающих мультипликативный порядок на одночленах.

Напомним, что *аннулятором* множества $\chi \subseteq R$ называется идеал $\mathrm{An}(\chi) = \{s \in R \mid \chi s = 0\}$.

Предложение 2. *Пусть кольцо* R *допускает мультипликативный порядок. Тогда справедливы следующие утверждения*:

1) *для любых* $a, b \in R$ *или* $\mathrm{An}(a) \subseteq \mathrm{An}(b)$, *или* $\mathrm{An}(b) \subseteq \mathrm{An}(a)$, *т. е. аннуляторы элементов из* R *образуют цепь в решётке идеалов* R;
2) 0 *и* 1 *— единственные идемпотенты в* R;
3) *если к тому же кольцо* R *артиново, то оно локально.*

Доказательство. Докажем первое утверждение. Пусть $\prec$ — мультипликативный порядок на $[R, X]$. Порядок $\prec$ разделяет мономы, поэтому для любых $a, b \in R \setminus 0$ или $ae \prec bx_1$, или $bx_1 \prec ae$. Отсюда ввиду (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, так как $\mathrm{An}(0) = R$.

Докажем утверждение 2). Пусть в R существует идемпотент $f \notin \{0, 1\}$. Положим $g = 1 - f$, тогда f, g — не равные 0 ортогональные идемпотенты. Аннуляторы $\mathrm{An}(f) = (g)$ и $\mathrm{An}(g) = (f)$ несравнимы, что противоречит утверждению 1).

Третье утверждение следует из второго. □

Следующий пример показывает, что из того, что выполнено утверждение 3) (или утверждение 2)) предложения 2, не следует, что R допускает мультипликативный порядок.

Пример 3. Пусть $I = (x^2, y^2) \lhd \mathbb{Z}_2[x, y]$. Положим $R = \mathbb{Z}_2[x, y]/I = \mathbb{Z}_2[\bar{x}, \bar{y}]$, где $\bar{x} = x + I$ и $\bar{y} = y + I$. Очевидно, что R — локальное артиново кольцо. Вместе с тем аннуляторы $\mathrm{An}(\bar{x}) = (\bar{x})$ и $\mathrm{An}(\bar{y}) = (\bar{y})$ несравнимы. Согласно пункту 1) предложения 2 кольцо R не допускает мультипликативного порядка на одночленах.

В настоящий момент неизвестно, следует ли из условия 1) предложения 2 наличие мультипликативного порядка на $[R, X]$.

Построение мультипликативных порядков

Транзитивное рефлексивное отношение называется *предпорядком*. Пусть на R задан некоторый предпорядок $\lesssim$. Вместе с ним всегда предполагаются заданными отношение эквивалентности $\sim$ и порядок $<$:

$$a \sim b \iff (a \lesssim b) \,\&\, (b \lesssim a),$$
$$a < b \iff (a \lesssim b) \,\&\, (a \not\sim b).$$

Важным примером предпорядка на R является *аннуляторный предпорядок* $\lesssim_{\mathrm{An}}$. Для любых $a, b \in R$

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

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

Всякий порядок $\prec$ на $[X]$ может быть продолжен до порядка на $[R, X]$ с помощью предпорядка $\lesssim$ на R. А именно, для любых $a, b \in R \setminus 0$ и $u, v \in [X]$ полагают

$$au \prec bv \overset{\mathrm{def}}{\iff} \begin{cases} a < b \text{ или} \\ a \sim b \text{ и } u \prec v. \end{cases} \tag{4}$$

Теорема 4. *Отношение $\prec$, определённое формулой* (4), *задаёт на $[R, X]$ мультипликативный порядок тогда и только тогда, когда выполнены следующие условия*:

1) *$\prec$ — линейный, согласованный с умножением* (*т. е. для любых $u, v, w \in [X]$ из $u \prec v$ следует, что $uw \prec vw$*) *порядок на $[X]$*;
2) *для любых $a, b \in R \setminus 0$ либо $a \lesssim b$, либо $b \lesssim a$, т. е. $\lesssim$ линеен на $R \setminus 0$*;
3) *для любых $a, b \in R \setminus 0$ из $a \lesssim b$ следует, что $a \lesssim_{\mathrm{An}} b$*;
4) *для любых $a, b, c \in R$, $ac, bc \neq 0$, $a \lesssim b$ тогда и только тогда, когда $ac \lesssim bc$.*

Доказательство. Докажем необходимость. Пусть определяемый формулой (4) порядок $\prec$ мультипликативен. Этот порядок разделяет мономы, поэтому для любых $u, v \in [X]$, $u \neq v$, или $1u \prec 1v$, или $1v \prec 1u$. Следовательно, исходный порядок $\prec$ на $[X]$ линеен. Также для любых $a, b \in R \setminus 0$ или $ae \prec bx_1$, или $bx_1 \prec ae$, откуда следует 2).

Пусть $u, v, w \in [X]$ и $u \prec v$, тогда $1u \prec 1v$ и согласно (2) $1uw \prec 1vw$. Значит, порядок $\prec$ на $[X]$ согласован с умножением. Пункт 1) доказан.

Пусть $a, b \in R \setminus 0$ и $a \lesssim b$. Ввиду уже доказанного найдутся такие мономы $u, v \in [X]$, что $u \prec v$. Тогда $au \prec bv$, и пункт 3) следует из (3).

Пусть $a, b, c \in R$ и $ac, bc \neq 0$. Возьмём мономы $u, v \in [X]$, такие что $u \prec v$. Если $a \lesssim b$, то $au \prec bv$ и ввиду (2) $acu \prec bcv$. Значит, $ac \lesssim bc$. Наоборот, если $b < a$, то $bv \prec au$ и $bcv \prec acu$, откуда следует, что $bc < ac$. Пункт 4) доказан.

Докажем достаточность. Пусть выполнены условия 1)—4). Из 1) и 2) следует, что $\prec$ разделяет мономы.

Из 4) следует, что для любых $a, b, c \in R$, $ac, bc \neq 0$, имеют место импликации $(a < b) \implies (ac < bc)$ и $(a \sim b) \implies (ac \sim bc)$. Ввиду этого определяемый формулой (4) порядок удовлетворяет условию (2).

Условие (3) вытекает из 3). Таким образом, согласно предложению 1 порядок $\prec$ на $[R, X]$ мультипликативен. $\square$

Все известные мультипликативные порядки задаются соотношением (4).

Следствие 5.

1. *Если на кольце R существует предпорядок $\lesssim$, удовлетворяющий условиям 1)—4) теоремы 4, то R допускает мультипликативный порядок.*
2. *Если аннуляторы элементов из R образуют цепь в решётке идеалов R и для любых $a, b, c \in R$ из $a <_{\mathrm{An}} b$ и $bc \neq 0$ следует $ac <_{\mathrm{An}} bc$, то R допускает мультипликативный порядок.*

Доказательство. Первое утверждение следует из теоремы 4. Достаточно взять произвольный линейный, согласованный с умножением порядок на $[X]$ (например, лексикографический) и продолжить его до мультипликативного порядка на $[R, X]$ по формуле (4).

Второе утверждение является следствием первого. При указанных предположениях условиям 2)—4) из теоремы 4 удовлетворяет предпорядок $\lesssim_{\mathrm{An}}$. $\square$

Следствие 6. *Кольца из следующих классов допускают мультипликативный порядок на одночленах*:

а) *области целостности*;

б) *локальные артиновы кольца главных идеалов*;

в) *локальные кольца, такие что* $[\mathrm{rad}(R)]^2 = 0$ ($\mathrm{rad}(R)$ — *радикал Джекобсона*).

Доказательство. Достаточно проверить, что для всех колец из указанных классов выполняются условия пункта 2 следствия 5. Эти условия легко проверить, используя явные формулы для аннуляторов.

В случае а) для всякого элемента $a \in R$

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

В случае б) идеалы кольца R образуют цепь

$$R > \pi R > \pi^2 R > \ldots > \pi^{n-1} R > \pi^n R = 0, \tag{5}$$

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 $n = 1$). Всякий элемент $a \in R$ можно представить в виде $a = \alpha\pi^i$, $\alpha \in R^*$, $i \in \overline{0, n}$, при этом

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

Рассмотрим случай в). Если $J = \mathrm{rad}(R) = 0$, то R — поле и утверждение следует из а). Пусть $J \neq 0$, тогда для любого $a \in R$

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

Отметим, что существуют кольца, допускающие мультипликативный порядок на мономах и не принадлежащие ни одному из указанных в следствии 6 классов.

Пример 7 ([1]). Пусть P — поле, $P[x_1, \ldots, x_k]$ — кольцо полиномов и $I = (x_1, \ldots, x_k)^m$. Положим $R = P[X]/I$. Тогда R — локальное артиново кольцо, допускающие мультипликативный порядок. Вместе с тем при $m > 2$ R содержит делители нуля, не является кольцом главных идеалов и $[\mathrm{rad}(R)]^2 \neq 0$.

В связи с пунктом б) следствия 6 представляет интерес следующая теорема.

Теорема 8 ([1]). *Пусть R — коммутативное квазифробениусово кольцо. Кольцо R допускает мультипликативный порядок на одночленах в том и только том случае, когда R — локальное артиново кольцо главных идеалов.*

Следующий пример показывает, что условия из пункта 2 следствия 5 не являются необходимыми для существования на $[R, X]$ мультипликативного порядка.

Пример 9. Пусть P — поле, $P[x, y]$ — кольцо полиномов и $I = (x^2, xy^2, y^3)$. Положим $R = P[x, y]/I = P[\bar{x}, \bar{y}]$, здесь $\bar{x} = x + I$ и $\bar{y} = y + I$. R — артиново локальное кольцо, радикал Джекобсона J равен $(\bar{x}, \bar{y})$,

$$R = \{\alpha + \beta\bar{x} + \gamma\bar{y} + \delta\bar{x}\bar{y} + \varepsilon\bar{y}^2 \mid \alpha, \beta, \gamma, \delta, \varepsilon \in P\}.$$

Для элемента $a = \alpha + \beta\bar{x} + \gamma\bar{y} + \delta\bar{x}\bar{y} + \varepsilon\bar{y}^2$ из R имеет место равенство

$$\mathrm{An}(a) = \begin{cases} 0 & \text{при } \alpha \neq 0, \\ J^2 & \text{при } \alpha = 0,\ \gamma \neq 0, \\ J^2 + (\bar{x}) & \text{при } \alpha = \gamma = 0,\ \beta \neq 0, \\ J & \text{при } \alpha = \gamma = \beta = 0,\ \delta\varepsilon \neq 0, \\ 0 & \text{при } \alpha = \gamma = \beta = \delta = \varepsilon = 0. \end{cases}$$

Из последнего соотношения следует, что $\bar{x} <_{\mathrm{An}} \bar{y}$, но $\bar{x}\bar{y} \sim_{\mathrm{An}} \bar{y}^2$. Таким образом, для R не выполняется второе условие из пункта 2 следствия 5.

Вместе с тем можно проверить, что определяемый соотношением

$$a \lesssim b \overset{\text{def}}{\Longleftrightarrow} \begin{cases} a \lesssim_{\mathrm{An}} b \text{ и не } a \sim b \sim \bar{x}\bar{y} \text{ или} \\ a \sim b \sim \bar{x}\bar{y}, \ a \in P^*\bar{x}\bar{y} + P\bar{y}^2 \text{ и } b \in P\bar{x}\bar{y} + P^*\bar{y}^2 \end{cases}$$

предпорядок на R удовлетворяет всем условиям из пункта 1 следствия 5, и значит, R допускает мультипликативный порядок на одночленах.

Вопрос о том, следует ли из условий пункта 1 следствия 5 наличие мультипликативного порядка на $[R, X]$, остаётся открытым.

Литература

[1] Горбатов Е. В. Стандартные базисы, согласованные с нормированием, и вычисления в идеалах и полилинейных рекуррентах // Фундамент. и прикл. мат. — 2004. — Т. 10, вып. 3. — С. 23—71.

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

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

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

[5] 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.

[6] 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.

[7] Adams W., Loustaunau P. An Introduction to Gröbner Bases. — Amer. Math. Soc., 1994. — (Grad. Stud. Math.; Vol. 3).