ISSN 2181-3187

ЗАДАЧА О ПРИНАДЛЕЖНОСТИ ПОЛИНОМА $f[x_1, x_2, \dots, x_n]$ ИДЕАЛУ $I \subset k[x_1, x_2, \dots, x_n]$

Хабибова Амира Улугбековна
Самаркандский государственный университет,
Факультет математики магистрант

Аннотация: В этой статье рассматривается задача о принадлежности полинома f идеалу $I \subset k[x_1, x_2, \dots, x_n]$. Данная задача легко решается с помощью базисов Гребнера и алгоритма деления многочленов нескольких переменных. Базисы Гребнера легко построить используя компьютерные программы. Метод базисов Гребнера реализован в достаточно мощных компьютерных системах.

Ключевые слова: полиномиальные идеалы, базисы Гребнера, алгоритм деления, мономиальное упорядочение.

Определение 1. Пусть $I \subset k[x_1, x_2, \dots, x_n]$-ненулевой идеал.

1) Обозначим через LT(I) множество старших членов элементов из I, т.е. LT(I)={cx^α: существует $f \in I$ и LT(f)=cx^α}.

2) Обозначим через <LT(I)> идеал, порожденный элементами из LT(I).

Пусть I конечно порожден, то есть $I =< f_1, f_2, \dots, f_s >$. Тогда <LT($f_1$), ..., LT($f_s$) > и <LT(I)> могут быть *разными* идеалами. Конечно, LT(f_i)$\in$ LT(I)$\subset$<LT(I)>; Поэтому <LT(f_1), ..., LT(f_s) > $\subset$<LT(I)>. Однако <LT(I)> может быть строго больше.

Определение 2. Бинарное отношение $>$ на $Z_{\geq 0}^n$, которое обладает следующими свойствами:

1) $>$ является линейным упорядочением на $Z_{\geq 0}^n$.

2) если $\alpha > \beta$ и $\gamma \in Z_{\geq 0}^n$, то $\alpha + \gamma > \beta + \gamma$;

3) $>$ вполне упорядочивает $Z_{\geq 0}^n$, т.е. любое непустое подмножество в $Z_{\geq 0}^n$ имеет минимальный (наименьший) элемент (по отношению к упорядочиванию $>$)

называется мономиальным упорядочением на $k[x_1, x_2, \dots, x_n]$.

Определение 3. (*лексикографическое упорядочение*). Пусть

Пусть $\alpha = (\alpha_1, \dots \alpha_n), \beta = (\beta_1, \dots \beta_n) \in Z_{\geq 0}^n$.Тогда $\alpha >_{lex} \beta$, если самая левая ненулевая координата вектора $\alpha - \beta \in Z_{\geq 0}^n$ положительна. То есть $x^\alpha >_{lex} x^\beta$, если $\alpha >_{lex} \beta$.

Определение 4. (*градуированное лексикографическое упорядочение*). Пусть $\alpha, \beta \in Z_{\geq 0}^n$. Тогда $\alpha >_{grlex} \beta$, если

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i \text{ или } |\alpha| = |\beta| \text{ и } \alpha >_{lex} \beta$$

ISSN 2181-3187

То есть сначала мономы упорядочиваются по полной степени, а если полные степени равны, то переходится к лексикографическому упорядочению.

Определение 5. (*градуированное обратное лексикографическое упорядочение*). Пусть $\alpha, \beta \in Z_{\geq 0}^{n}$. Тогда $\alpha >_{grevlex} \beta$, если

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

или $|\alpha| = |\beta|$ и самая правая ненулевая координат

Определение 6. Пусть задано мономиальное упорядочение. Конечное подмножество $G = \{g_1, \dots, g_s\}$ элементов идеала I называется его базисом Гребнера (или стандартным базисом), если

$$<\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)>=<\mathrm{LT}(I)>.$$

Или другими словами, множество $\{g_1, \dots, g_s\} \subset \mathrm{I}$ называется базисом Грёбнера идеала I в том и только в том случае, когда старший член любого элемента из I делится на хотя бы один старший член $LT(g_i)$.

Утверждение 1. Пусть задано некоторое мономиальное упорядочение. Тогда любой ненулевой идеал $\mathrm{I} \subset \mathrm{k}[\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I является его базисом.

Предложение 1. Пусть $G = \{g_1, \dots, g_s\}$ -базис Грёбнера идеала $I \subset k[x_1, x_2, \dots, x_n]$, и пусть $f \in k[x_1, x_2, \dots, x_n]$. Тогда существует единственный полином $r \in k[x_1, x_2, \dots, x_n]$, который обладает следующими свойствами:

1) ни один член полинома r не делится ни на один из старших членов $<\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)>$;

2) существует $g \in I$, такой, что $f = g + r$.

То есть является остатком от деления f на G, не зависящим от порядка делителей в G.

Остаток r называется *нормальной формой* полинома f.

Следствие 1. Пусть $G = \{g_1, \dots, g_s\}$-базис Грёбнера идеала $I \subset k[x_1, x_2, \dots, x_n]$, и пусть $f \in k[x_1, x_2, \dots, x_n]$. Тогда $f \in I$ в том и только в том случае, когда остаток от деления f на G равен нулю.

Доказательство. Если остаток равен нулю, то, как уже отмечалось, $f \in I$. Обратно, пусть $f \in I$. Тогда равенство $f = f + 0$ удовлетворяет обоим условиям предложения 2.3. Из единственности представления полинома f в таком виде следует, что 0 является остатком от деления f на G.ка.

При помощи базисов Грёбнера и алгоритма деления строится следующий алгоритм решения задачи о принадлежности идеалу $I =< f_1, \dots, f_s >$ полинома f: сначала строится базис Гребнера $G = \{g_1, \dots, g_t\}$ для идеала I, затем при помощи алгоритма деления делим полином f на множество образующих базиса Гребнера $G = \{g_1, \dots, g_t\}$;

ISSN 2181-3187

Тогда $f \in I$ в том и только в том случае, когда $\bar{f}^G = 0$.

Пример 1. Пусть $I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 > \subset C[x,y,z]$, и пусть используется grlex-упорядочение. Рассмотрим полином $f = -4x^2y^2z^2 + y^6 + 3z^5$. Верно ли, что $f \in I$?

Сначала проверим является ли множество образующих базисом Грёбнера.

$I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 > \subset C[x,y,z]$, grlex-упорядочение,

$f_1 = xz - y^2$, $f_2 = x^3 - z^2$, $f_1, f_2 \in C[x,y,z]$

Так как $\alpha = (1,0,1)$, $\beta = (3,0,0) \Rightarrow \gamma = (3,0,1)$.

$\Rightarrow S(f_1,f_2) = \frac{x^3z}{xz} \cdot f_1 - \frac{x^3z}{x^3} \cdot f_2 = x^2(xz - y^2) - z(x^3 - z^2) = x^3z - x^2y^2 - x^3z + z^3 = -x^2y^2 + z^3$;

$I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 >$, $S(f_1,f_2) = -x^2y^2 + z^3 \in I$ и остаток от деления $(-x^2y^2 + z^3)$ на $F = \{f_1, f_2\}$ равен $-x^2y^2 + z^3 \neq 0$. Отсюда следует, что множество образующих не является базисом Гребнера.

Добавим остаток $f_3 = -x^2y^2 + z^3$ в порождающее множество.

Теперь $F = \{f_1, f_2, f_3\}$.

Применим критерий того, что базис идеала является базисом Грёбнера (Th. G).

Имеем $S(f_1,f_2) = -x^2y^2 + z^3 = f_3$, значит $\overline{S(f_1,f_2)}^F = 0$.

Вычислим $S(f_1,f_3)$. Так как $\alpha = (1,0,1)$, $\beta = (2,2,0) \Rightarrow \gamma = (2,2,1)$.

$\Rightarrow \quad S(f_1,f_3) = \frac{x^2y^2z}{xz} \cdot f_1 - \frac{x^2y^2z}{(-x^2y^2)} \cdot f_3 = xy^2(xz - y^2) + z(-x^2y^2 + z^3) = x^2y^2z - xy^4 - x^2y^2z + z^4 = -xy^4 + z^4$, но $\overline{S(f_1,f_3)}^F = -xy^4 + z^4 \neq 0$.

Следовательно, мы должны добавить остаток $f_4 = -xy^4 + z^4$ к порождающему множеству, т.е. $F = \{f_1, f_2, f_3, f_4\}$. Имеем

$$\overline{S(f_1,f_2)}^F = \overline{S(f_1,f_3)}^F = 0.$$

Вычислим $S(f_1,f_4)$. Так как $\alpha = (1,0,1)$, $\beta = (1,4,0) \Rightarrow \gamma = (1,4,1)$.

$\Rightarrow S(f_1,f_4) = \frac{xy^4z}{xz} \cdot f_1 - \frac{xy^4z}{(-xy^4)} \cdot f_4 = y^4(xz - y^2) + z(-xy^4 + z^4) = xy^4z - y^6 - xy^4z + z^5 = -y^6 + z^5$.

Следовательно, мы должны добавить остаток $f_5 = -y^6 + z^5$ к порождающему множеству, т.е. $F = \{f_1, f_2, f_3, f_4, f_5\}$. Имеем

$$\overline{S(f_1,f_2)}^F = \overline{S(f_1,f_3)}^F = \overline{S(f_1,f_4)}^F = 0.$$

Вычислим $S(f_1,f_5)$. Так как $\alpha = (1,0,1)$, $\beta = (0,6,0) \Rightarrow \gamma = (1,6,1)$.

$\Rightarrow S(f_1,f_5) = \frac{xy^6z}{xz} \cdot f_1 - \frac{xy^6z}{(-y^6)} \cdot f_5 = y^6(xz - y^2) + xz(-y^6 + z^5) = xy^6z - y^8 - xy^6z + xz^6 = xz^6 - y^8 = z^5 \cdot f_1 - y^2 \cdot f_5$.

$\Rightarrow \overline{S(f_1,f_5)}^F = 0$.

ISSN 2181-3187

Вычислим $S(f_2, f_3)$. Так как $\alpha = (3,0,0),\ \beta = (2,2,0) \Rightarrow \gamma = (3,2,0)$.

$\Rightarrow \quad S(f_2, f_3) = \frac{x^3y^2}{x^3} \cdot f_2 - \frac{x^3y^2}{(-x^2y^2)} \cdot f_3 = y^2(x^3 - z^2) + x(-x^2y^2 + z^3) = x^3y^2 - y^2z^2 - x^3y^2 + xz^3 = xz^3 - y^2z^2 = z^2 \cdot f_1.$

$\Rightarrow$ легко проверить, что $\overline{S(f_2, f_3)}^F = 0.$

Вычислим $S(f_2, f_4)$. Так как $\alpha = (3,0,0),\ \beta = (1,4,0) \Rightarrow \gamma = (3,4,0)$.

$\Rightarrow S(f_2, f_4) = \frac{x^3y^4}{x^3} \cdot f_2 - \frac{x^3y^4}{(-xy^4)} \cdot f_4 = y^4(x^3 - z^2) + x^2(-xy^4 + z^4) = x^3y^4 - y^4z^2 - x^3y^4 + x^2z^4 = x^2z^4 - y^4z^2 = (xz^3 + y^2z^2) \cdot f_1.$

$\Rightarrow$легко вычислить, что $\overline{S(f_2, f_4)}^F = 0.$

Вычислим $S(f_2, f_5)$. Так как $\alpha = (3,0,0),\ \beta = (0,6,0) \Rightarrow \gamma = (3,6,0)$.

$\Rightarrow S(f_2, f_5) = \frac{x^3y^6}{x^3} \cdot f_2 - \frac{x^3y^6}{(-y^6)} \cdot f_5 = y^6(x^3 - z^2) + x^3(-y^6 + z^5) = x^3y^6 - y^6z^2 - x^3y^6 + x^3z^5 = x^3z^5 - y^6z^2 = (x^2z^4 + xy^2z^3 + y^4z^2) \cdot f_1.$

$\Rightarrow$ легко проверить, что $\overline{S(f_2, f_5)}^F = 0.$

Вычислим $S(f_3, f_4)$. Так как $\alpha = (2,2,0),\ \beta = (1,4,0) \Rightarrow \gamma = (2,4,0)$.

$\Rightarrow S(f_3, f_4) = \frac{x^2y^4}{(-x^2y^2)} \cdot f_3 - \frac{x^2y^4}{(-xy^4)} \cdot f_4 = -y^2(-x^2y^2 + z^3) + x(-xy^4 + z^4) = x^2y^4 - y^2z^3 - x^2y^4 + xz^4 = xz^4 - y^2z^3 = z^3 \cdot f_1.$

$\Rightarrow$ легко вычислить, что $\overline{S(f_3, f_4)}^F = 0.$

Вычислим $S(f_3, f_5)$. Так как $\alpha = (2,2,0),\ \beta = (0,6,0) \Rightarrow \gamma = (2,6,0)$.

$S(f_3, f_5) = \frac{x^2y^6}{(-x^2y^2)} \cdot f_3 - \frac{x^2y^6}{(-y^6)} \cdot f_5 = -y^4(-x^2y^2 + z^3) + x^2(-y^6 + z^5) = x^2y^6 - y^4z^3 - x^2y^6 + x^2z^5 = x^2z^5 - y^4z^3 = (xz^4 + y^2z^3) \cdot f_1.$

$\Rightarrow$ легко вычислить, что $\overline{S(f_3, f_5)}^F = 0.$

Вычислим $S(f_4, f_5)$. Так как $\alpha = (1,4,0),\ \beta = (0,6,0) \Rightarrow \gamma = (1,6,0)$.

$S(f_4, f_5) = \frac{xy^6}{(-xy^4)} \cdot f_4 - \frac{xy^6}{(-y^6)} \cdot f_5 = -y^2(-xy^4 + z^4) + x(-y^6 + z^5) = xy^6 - y^2z^4 - xy^6 + xz^5 = xz^5 - y^2z^4 = z^4 \cdot f_1.$

$\Rightarrow$ легко проверить, что $\overline{S(f_4, f_5)}^F = 0.$

Таким образом, $\overline{S(f_i, f_j)}^F = 0$ для $1 \le i \le j \le 5$ и $F = (f_1, f_2, f_3, f_4, f_5).$

$\Rightarrow \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, -x^2y^2 + z^3, -xy^4 + z^4, -y^6 + z^5\}$ – базис Грёбнера

Используя компьютерную систему получаем:

$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = 0 \cdot f_1 + 0 \cdot f_2 - 4z^2 f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Так как остаток от деления равен нулю, то $f \in I.$

ISSN 2181-3187

В качестве другого примера возьмем $f = xy - 5z^2 + x$. Здесь очевидно, что $f \notin I$. Так как LT(f)= xy не принадлежит идеалу $< LT(G) >=< xz, x^3, x^2y^2, xy^4, y^6 >$, т.е. $\bar{f}^G \neq 0$, так что $f \notin I$.

Пример 2. Пусть $I =< f_1, f_2 >=< -x^3 + y,\ x^2y - z >\subset C[x, y, z]$, и пусть используется lex-упорядочение. Рассмотрим полином

$f = xy^3 + y^5 - z^3 - z^2$. Верно ли, что $f \in I$?

Множество образующих не является базисом Грёбнера. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I. Используя компьютерную систему Maple 2021, получаем:

```
> F := {-x^3+y, x^2*y-z};
```

$$F := \{-x^3 + y, x^2 y - z\}$$

```
> GB_F:= Basis(F, plex (x, y, z));
```

$$GB\_F := [y^5 - z^3, xz - y^2, xy^3 - z^2, x^2 y - z, x^3 - y]$$

$G = \{f_1, f_2, f_3, f_4, f_5\} = \{y^5 - z^3, xz - y^2,\ xy^3 - z^2,\ x^2y - z, x^3 - y\}$.

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = 0 \cdot f_1 + 0 \cdot f_2 + 1 \cdot f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Так как остаток от деления равен нулю, то $f \in I$.

Пример 3. Необходимо выяснить, принадлежит ли полином $f = x^3z - 2y^2$ идеалу

$I =< f_1, f_2, f_3 >=< xz - y, xy + 2z^2, y - z >\subset C[x, y, z]$.

Множество образующих не является базисом Грёбнера. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I. Используя компьютерную систему, получаем

$$G = \{f_1, f_2, f_3\} = \{xz - z, y - z, 2z^2 + z\}.$$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = (x^2 + x + 1) \cdot f_1 + (-2y - 2z) \cdot f_2 - 1 \cdot f_3 + 2z.$$

Так как остаток от деления равен $2z$, то $f \notin I$.

Литература

1. Аржанцев И.В. Базисы Грёбнера и системы алгебраических уравнений// М. Ж. МЦНМО, 2003.

2. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. – М.:Мир,2000.