Базисы Гребнера

Емиж И.Т.

Во многих задачах коммутативной алгебры возникают вопросы о принадлежности многочлена от нескольких переменных к тому или иному идеалу. Одним из инструментов проверки является базис Гребнера.

1 Многочлены от одной переменной

Напомним, что кольцо многочленов $F[x]$ является Евклидовым, то есть целостным кольцом в котором задана функция $deg(f)$

$$deg : F[x] \setminus 0 \to N_0$$

Удовлетворяющая свойствам:

1. $deg(ab) \geq deg(a)$, причем равенство имеет место тогда и только тогда, когда элемент b обратим.

2. Для любых $a, b \in F[x]$, где $b \neq 0$, существуют такие $q, r \in F[x]$, что $a = qb + r$, где либо $r = 0$, либо $deg(r) < deg(b)$.

То есть в данном кольце существует деление с остатком и соответственно алгоритм Евклида. Следовательно справедливо

Предложение 1.1. *Кольцо $F[x]$ является кольцом главных идеалов. (то есть каждый идеал порожден некоторым элементом)*

2 Деление многочленов от нескольких переменных

Чтобы определить деление с остатком нужно ввести некоторый порядок на мономах. Далее будем считать, что порядок на мономах введен лексикографически, то есть моном $x^\alpha = x^{\alpha_1}...x^{\alpha_n}$ старше монома $x^\beta = x^{\beta_1}...x^{\beta_n}$, если $\alpha_1 = \beta_1, ..., \alpha_k = \beta_k, \alpha_{k+1} > \beta_{k+1}$.

Пусть $f = a_\alpha x^\alpha + ...$ и $g = b_\beta x^\beta + ...$, где $a_\alpha x^\alpha$ и $b_\beta x^\beta$ старшие члены соответствующих многочленов, если некоторый член $c_\gamma x^\gamma$ многочлена f делится на $b_\beta x^\beta$, положим $f_1 = f - \frac{c_\gamma x^\gamma}{b_\beta x^\beta} g$, применим к f_1 такое же преобразование и т.д.

Аналогично можно определять деление с остатком многочлена f на несколько многочленов $f_1, f_2, ..., f_s$. В результате получим представление $f = u_1 f_1 + u_2 f_2 + ... + u_s f_s + r$, где у многочлена r нет членов делящихся на старшие мономы многочленов $f_1, f_2, ..., f_s$. В таком случае будем говорить, что r – остаток от деления f на многочлены $f_1, f_2, ..., f_s$.

Пример 2.1. *Рассмотрим кольцо многочленов* $\mathbb{R}[x_1, x_2]$. *Пусть* $f = x_1^2 + x_2^2$ *и* $f_1 = x_1^2 + x_2$, $f_2 = x_1 + x_2$. *Тогда справедливы равенства*

$$f = 1 \cdot f_1 + 0 \cdot f_2 + x_2^2 - x_2$$

$$f = 0 \cdot f_1 + (x_1 - x_2) f_2 + 2x_2^2$$

то есть такой остаток определен не однозначно. (Одно из возможных определений базиса Гребнера как раз и заключается в том, что остаток любого многочлена f *на данный базис определен однозначно)*

Определение 2.2. *Будем говорить, что (ненулевые) многочлены* $g_1, g_2, ..., g_t \in I$ *образуют базис Гребнера идеала* I, *если у любого (ненулевого) многочлена* $f \in I$ *старший член делится на старший член одного из многочленов* $g_1, ..., g_t$.

Теорема 2.3. *Многочлены* $g_1, g_2, ..., g_t$ *образуют базис Гребнера идеала* I *тогда и только тогда, когда выполняется одно из следующих эквивалентных условий:*

1. $f \in I \Leftrightarrow$ *остаток от деления на* $g_1, g_2, ..., g_t$ *равен 0;*

2. $f \in I \Leftrightarrow \sum h_i g_i$ *и старший моном многочлена* f *равен старшему из произведений старших мономов* $h_i g_i$*;*

3. *Идеал* $L(I)$, *порожденный старшими членами элементов идеала* I, *порожден старшими членами многочленов* $g_1, g_2, ..., g_t$.

Теперь возникает вопрос, как выяснить за конечное число шагов, является ли данный набор базисом Гребнера и как находить эти базисы. Одним из таких алгоритмов является алгоритм Бухбергера.

Пусть $f = a_\alpha x^\alpha + ...$ и $g = b_\beta x^\beta + ...$ и x_γ – НОК мономов $a_\alpha x^\alpha$ и $b_\beta x^\beta$. Положим $S(f, g) = \frac{x_\gamma}{a_\alpha x^\alpha} f - \frac{x_\gamma}{b_\beta x^\beta} g$.

Теорема 2.4 (Бухбергер)**.** *Многочлены* $g_1, g_2, ..., g_t$ *образуют базис Гребнера тогда и только тогда, когда при всех* $i \neq j$ *остаток от деления многочлена* $S(g_i, g_j)$ *на* $g_1, g_2, ..., g_t$ *равен нулю.*

С помощью данной теоремы можно показать, что следующий алгоритм позволяет найти базис Гребнера идеала, порожденного многочленами $f_1, ..., f_s$.

Вычислим остатки от деления многочленов $S(f_i, f_j)$ на $f_1, ..., f_s$ и добавим все ненулевые остатки к набору $f_1, ..., f_s$. Повторим и т.д. Ясно, что эта процедура завершается за конечное число шагов, а согласно предыдущей теореме мы получим базис Гребнера.

Список литературы

[1] Adams W. W., Loustaunau P. An introduction to Gröbner bases. – American Mathematical Society, 2022. – Т. 3.

[2] Buchberger B., Winkler F. (ed.). Gröbner bases and applications. – Cambridge University Press, 1998. – Т. 251.