ЗАДАЧА О ПРИНАДЛЕЖНОСТИ ИДЕАЛУ

Каримова Мафтуна
Специальность: 5А130101-Математика (по направлениям)
2-курс

Алгоритм деления для полиномов от одной переменной может быть применен для решения задачи о принадлежности идеалу. Для решения этой задачи в случае нескольких переменных необходимо обобщить алгоритм деления в $k[x]$ на общий случай полиномиального кольца $k[x_1, \dots, x_n]$. В этой работе описан алгоритм деления в кольце $k[x_1, \dots, x_n]$ т.е. представить полином f из этого кольца в виде

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

где «частные» $a_1, \dots, a_s$ и остаток r принадлежат $k[x_1, \dots, x_n]$.

Определение 1. *Мономиальным упорядочением* на $k[x_1, \dots, x_n]$ называется любое бинарное отношение $>$ на $Z_{\geq 0}^n$, обладающее следующими свойствами:

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

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

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

Определение 2. (лексикографическое упорядочение). Пусть $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in Z_{\geq 0}^n$. Мы говорим, что $\alpha >_{\text{lex}} \beta$, если самая левая ненулевая координата вектора $\alpha - \beta \in Z_{\geq 0}^n$ положительна. Мы будем писать $x^\alpha >_{lex} x^\beta$, если $\alpha >_{lex} \beta$.

Основная идея алгоритма та же, что и в случае одной переменной: мы должны уничтожать старший член полинома f (определенный заданным мономиальным упорядочением), умножая некоторый f_i на подходящий моном и вычитая. Этот моном будет членом соответствующего a_i.

Теорема. (алгоритм деления в $k[x_1, \dots, x_n]$). *Зафиксируем некоторое мономиальное упорядочение $>$ на $Z_{\geq 0}^n$, и пусть $F = (f_1, \dots, f_s)$ - упорядоченный s-набор полиномов из $k[x_1, \dots, x_n]$. Тогда любой полином $f \in k[x_1, \dots, x_n]$ можеть быть записан в виде*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

где a_i, $r \in k[x_1, \ldots, x_s]$ *и или r = 0, или r есть линейная комбинация мономов (с коэффициентами из k), ни один из которых не делится ни на один из старших членов* $LT(f_1)$, ...,$LT(f_s)$. *Мы называем r* остатком *от деления полинома* f *на F. Более того, если* $a_i f_i \neq 0$, *то*

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i).$$

Первым важным свойством алгоритма деления в $k[x]$ является то, что остаток определен однозначно. Покажем на примере, что в случае нескольких переменных это свойство не выполняется.

Пример 1. Поделим $f = x^7y^2 + x^3y^2 - y + 1$ на $f_1 = x - y^3$ и на $f_2 = xy^2 - x$. Мы используем lex-упорядочение с $x > y$. Если проведем деление сами, то получим

$$x^7y^2 + x^3y^2 - y + 1 = \\ = (x - y^3)(x^6y^2 + x^5y^5 + x^4y^8 + x^3y^{11} + x^2y^{14} + x^2y^2 + xy^{17} + xy^5 \\ + y^{20} + y^8) + (xy^2 - x)0 + y^{23} + y^{11} - y + 1$$

Пример 2. Этот пример отличается от примера 1.1. только переменой порядка делителей. Если мы сравним пример 1.1. с примером 1.2., то увидим, что полученный нами остаток не равен остатку в примере

$$x^7y^2 + x^3y^2 - y + 1 = (x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + \\ + 2)(xy^2 - x) + (x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2)(x - y^3) + 2y^3 - y + 1$$

Этот пример показывает, что остаток r не определен однозначно требовании-ем, чтобы ни один его член не делился ни на один из $LT(f_1), \ldots, LT(f_s)$.

Важным достоинством алгоритма деления в $k[x]$ является возможность с его помощью решать задачу о принадлежности идеалу. Обладает ли подобным свойством обобщенный алгоритм деления? Вот простое следствие теоремы: если остаток от деления f на $F = (f_1, \ldots, f_s)$ равен нулю, $r = 0$, т.е.

$$f = a_1f_1 + \cdots + a_sf_s,$$

то $f \in < f_1, \ldots, f_s >$. Другими словами, $r = 0$ - это *достаточное* условие принадлежности идеалу. Следующий пример показывает, однако, что $r = 0$ не является *необходимым* условием.

Пример 3. Пусть $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x,y]$ с lex-упорядочением. Если мы разделим $f = xy^2 - x$ на $F = (f_1, f_2)$, то в результате получим

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y).$$

С другой стороны, деля f на $F = (f_1, f_2)$, получаем

$$xy^2 - x = x(xy + 1) + 0(xy + 1) + 0.$$

Из второго равенства следует, что $f \in < f_1, f_2 >$. Но тогда первое равенство демонстрирует, что, хотя f и принадлежит идеалу $< f_1, f_2 >$, остаток от деления f на F не равен нулю.

Таким образом, алгоритм деления, определенный теоремой, является несовершенным обобщением алгоритма деления в $k[\mathrm{x}]$. Чтобы исправить ситуацию, следует вспомнить об одном правиле: если мы работаем с набором полиномов $f_1, f_2, \ldots, f_s \in k[x_1, \ldots, x_n]$, то следует рассматривать идеал I, ими порожденный. Другими словами, следует рассматривать и другие наборы полиномов, порождающие тот же идеал. Можно сформулировать естественную задачу: существует ли для произвольного идеала I «хорошее» порождающее множество, т.е. такое, что остаток r от деления на множество «хороших» образующих элементов был бы однозначно определен и условие $r = 0$ было бы *необходимым* и *достаточным* условием принадлежности идеалу.

Литература

1. Кокс Д., Литлл Дж., Оши Д. Идеалы, многообразия и алгоритмы.- М.: Мир, 2000.

2. Ван дер Варден Б.Л. Алгебра. – М.:Наука,1979.

3. Ленг С. Алгебра.-М.:Мир,1968.

Научный руководитель:доц.У.Х.Нарзуллаев