10 Лекция 30.05

Базисы Гребнера Хотим научиться решать задачу вхождения: даны функции $f_1, \dots, f_k \in K[x_1, \dots, x_n]$; необходимо выяснить $f \in (f_1, \dots, f_k)$? Иными словами, существуют ли $n_1, \dots, n_k$, такие что $f = f_1 n_1 + \dots + f_k n_k$.

Рассмотрим частный случай при $n = 1$. Тогда любой идеал главный. Тогда $(f_1, \dots, f_k) = (d)$. Нужно проверить, что $d \mid f$.

Теперь при $k = 1$. Тогда нужно проверить, что $f \in (f_1) \Leftrightarrow f_1 \mid f$. Алгоритм следующий: сначала проверим, что $L(f_1) \mid L(f)$. Затем вычтем f_1 из f и продолжим процедуру дальше. Если в какой-то момент делимость не выполняется, то $f \notin (f_1)$.

Теперь попробуем обобщить алгоритм. Рассмотрим $\mathcal{F} = \{f_1, \dots, f_k\}$. Можно считать, что старшие коэффициенты f_i равны 1. Тогда $f_i = x^{b(i)} + \dots$, где под $x^{b(i)}$ следует понимать моном $x_1^{b(i)_1} \dots x_n^{b(i)_n}$. Пусть M_n — множество одночленов от $x_1, \dots, x_n$. Пусть $m \in M_n$ и $L(f_i) \mid m$. Определим оператор элементарной $\mathcal{F}$-редукции как $R_i^m : K[x_1, \dots, x_n] \to K[x_1, \dots, x_n]$. Задаем на базисе. Пусть $R_i^m(m) = m - \frac{m}{L(f_i)} f_i$. А при $m \neq m' : R_i^m(m') = m'$.

Оператор $\mathcal{F}$-редукции — это произвольная конечная композиция операторов $\mathcal{F}$-редукции.

Алгоритм деления Пусть $\mathcal{F} = \{f_1, \dots, f_k\}$, $f \in K[x_1, \dots, x_n]$. Представим $f = \lambda_1 x^{a(1)} + \dots + \lambda_p x^{a(p)}$. Считаем, что $\lambda_i \in K \setminus \{0\}$. Без ограничения общности считаем, что $x^{a(1)} > \dots > x^{a(p)}$. Будем называть это канонической формой f.

Шаг 1 Если $L(f_1) \mid x^{a(1)}$, то заменим $f = R_1^{x^{a(1)}}(f)$ и возвращаемся к шагу 1 опять. Сакральный смысл — каждый раз уменьшаем старший член.

Шаг 2 Если $L(f_1) \nmid x^{a(1)}$, но $L(f_2) \mid x^{a(1)}$, то заменяем $f = R_2^{x^{a(1)}}(f)$. И так далее. Если $L(f_1), \dots, L(f_k)$ не делят $x^{a(1)}$, то перейдем к $x^{a(2)}$ и повторим с шага 1.

Определение 57. *Одночлен $m \in M_n$ называется $\mathcal{F}$-нормальным, если $\forall i : L(f_i) \nmid m$. Многочлен $f \in K[x_1, \dots, x_n]$ называется $\mathcal{F}$-нормальным, если все его члены $\mathcal{F}$-нормальны.*

Понятно, что h является $\mathcal{F}$-нормальным $\Leftrightarrow R(h) = h$ для любого оператора редукции R.

Предложение 9. Алгоритм деления, примененный к некоторому многочлену f, остановится на нормальном многочлене $N(f) = N_{\mathcal{F}}(f)$ за конечное число шагов.

Доказательство. Пусть не останавливается. Тогда получается бесконечная последовательность строго убывающих лексикографически одночленов. Но тогда получаем противоречие с леммой, что в лексикографическом порядке не существует бесконечных убывающих цепочек. □

Определение 58. *Первой $\mathcal{F}$-нормальной формой многочлена f называется $N(f)$.*

Тогда нетрудно заметить, что $f \in (f_1, \dots, f_K) \Leftrightarrow N(f) = 0$.

Пример. Возьмем $f_1 = x_1^2 + x_2, f_2 = x_1^2 + x_3, f = x_2 - x_3$. Хотим проверить, что $f \in (f_1, f_2)$. Но тогда $N(f) = f$, что значит, что $f \notin (f_1, f_2)$. А это неправда, так как $f = f_1 - f_2$.

Алгоритм сломался. Починим его.

Определение 59. *Базисом Гребнера идеала $I = (f_1, \dots, f_k) \subseteq K[x_1, \dots, x_n]$ называется такое конечное множество $F = \{g_1, \dots, g_s\} \subseteq I$, такое что $\forall f \in I : \exists i : L(g_i) \mid L(f)$.*

Лемма 15. *Пусть $G \subseteq I$ — БГ. Тогда $N_G(f) = 0 \Leftrightarrow f \in I$.*

Доказательство. $\Rightarrow$. Если $N_G(f) = 0$, то $f - h_i g_i - h_j g_j - \dots = 0 \Rightarrow f \in (g_1, \dots, g_s) \subseteq I$.

Теперь $\Leftarrow$. Если $f \in I$, то $N_G(f) \in I$. Тогда $L(N_G(f)) \mid L(g_i)$. Но тогда нормальная форма не является нормальной. Получаем, что $N_G(f) = 0$. □

Предложение 10. Пусть $I \subseteq K[x_1, \dots, x_n]$ — идеал. Тогда верно:

1. БГ существует
2. Любой БГ является базисом идеала I

Доказательство. Сначала докажем 1. Воспользуемся леммой Диксона. Во множестве мономов $L(f), f \in I$ есть только конечное число минимальных элементов. Обозначим их $L(g_1), \dots, L(g_s)$. Но тогда $g_1, \dots, g_s$ — БГ.

Теперь докажем 2. Если $f \in I$, то $N_G(f) = 0$. поэтому $f \in (g_1, \dots, g_s)$. Следовательно $(g_1, \dots, g_s) \subseteq I$. Включение в обратную сторону верно по определению. □

Как построить базис Гребнера? Ответ простой — с помощью алгоритма Бухбергера.

Определение 60. *$\mathcal{F} = \{f_1, \dots, f_k\}$. Тогда $\mathcal{F}$-нормальной формой f называется $n(f)$, такой что $n(f)$ нормален и $n(f) = R(f)$, где R — оператор редукции.*

Определение 61. *Набор многочленов $G = \{g_1, \dots, g_s\}$ — БГ, если это БГ идеала $(g_1, \dots, g_s)$.*

Замечание 13. *Любой набор одночленов — БГ.*

Пусть L — множество таких одночленов f, у которых нормальная форма относительно $\mathcal{F}$ единственна.

Лемма 16. *$L \subseteq K[x_1, \dots, x_n]$ — подпространство.*

Доказательство. Понятно, что $L \neq \varnothing$, потому что $0 \in L$. Если $f \in L$, то и $\lambda f \in L$. Осталось показать, что L замкнуто относительно суммы. Мы докажем более сильное утверждение, что $n(g+h) = N(g) + N(h)$. По определению, $n(g+h) = R(g+h)$. Так как R линейный оператор, то $n(g+h) = R(g) + R(h)$. Так как все нормлальные формы для g совпадают, $\exists R'$, что $R'(R(g)) = N(g)$. Аналогично $\exists R''$, что $R''(R'(R(h))) = N(h)$. А тогда

$$R(g+h) = R''(R'(R(g+h))) = R''(R'(R(g))) + R''(R'(R(h))) = R''(N(g)) + N(h) = N(g) + N(h)$$

□

Определение 62. *Пусть $f_i, f_j \in K[x_1, \dots, x_n]$. Построим по ним S-многочлен.*

$$S(f_i, f_j) = m_{ij} f_i - m_{ji} f_j$$

где m_{ij}, m_{ji} взимно простые одночлены, такие что $m_{ij} L(f_i) = m_{ji} L(f_j)$.

Пример. Если $L(f_i) = x_1^2 x_2, L(f_j) = x_1^2 x_3$, то целесообразно взять $m_{ij} = x_3, m_{ji} = x_2$.

Замечание 14. *Старший член $S(f_i, f_j)$ может быть больше старших членов f_i, f_j.*

Пример. $f_i = x_1 x_3 + x_1 x_4, f_j = x_2 + x_4$. Тогда $m_{ij} = x_2, m_{ji} = x_1 x_3$, $S(f_i, f_j) = x_1 x_2 x_4$.

Теорема 15 (Критерий Бухбергера)**.** *Пусть $G = \{g_1, \dots, g_s\}$ — конечное подмножество в кольце многочленов $K[x_1, \dots, x_n]$. Тогда следующие условия эквивалентны:*

1. *G — БГ*
2. *$\forall i, j \, : \, N(S(g_i, g_j)) = 0$*
3. *$\forall i, j \, \exists$ оператор G-редукции, такой что $R(S(g_i, g_j)) = 0$*
4. *$\forall f \in K[x_1, \dots, x_n]$ все его G-нормальные формы одинаковы.*