11 Лекция 2.06

Доказательство критерия Бухбегера. $1 \to 2$. По определению $S(g_i, g_j) = m_{ij}g_i - m_{ji}g_j \in (g_1, \dots, g_s)$. Тогда по лемме $N(m_{ij}g_i - m_{ji}g_j) = 0$.

$2 \to 3$. $N(S(g_i, g_j)) = R(S(g_i, g_j)) = 0$.

$3 \to 4$. Хотим показать, что $L = K[x_1, \dots, x_n]$. Так как L подпространство, достаточно доказать, что все одночлены лежат в L. Пусть не так. Тогда $S \subseteq M_n$ — те мономы, которые не лежат в L (то есть те, у которых нормальная форма не единственна). Тогда найдется минимальный лексикографически элемент $m \in S$ (так как по лемме Диксона убывающие цепочки конечны). Пусть $R_1(m), R_2(m)$ — разные нормальные формы. Рассмотрим первые операторы, которые мы применили к m, пусть это $R_t^m(m), R_p^m(m)$ соответственно. Но тогда $R_1(m) = N(R_t^m(m))$, $R_2(m) = N(R_p^m(m))$ (потому что m минимальный). Сейчас мы хотим найти такое R', что $R'(R_t^m(m)) = R'(R_p^m(m))$, тогда мы получим противоречие, поскольку $N(R_t^m(m)) = N(R_p^m(m))$. Во-первых, $m = u_tL(g_t) = u_pL(g_p)$. Пусть $u = (u_t, u_p)$. Тогда $R_t^m(m) - R_p^m(m) = (m - u_tg_t) - (m - u_pg_p) = u_pg_p - u_tg_t = uS(g_p, g_t)$. Но по условию 3 существует такой оператор R'', что $R''(S(g_p, g_t)) = 0$. Разложим его как $R'' = R_{i_q}^{v_q} \dots R_{i_1}^{v_1}$. Возьмем $R' = R_{i_q}^{uv_q} \dots R_{i_1}^{uv_1}$. Наконец $R'(uS(g_p, g_t)) = 0 = R'(R_p^m(m) - R_t^m(m)) \Rightarrow R'(R_p^m(m)) = R'(R_t^m(m))$. Тогда $m \in L$, противоречие.

$4 \to 1$. Возьмем любой $f = h_1g_1 + \dots + h_sg_s$. Хотим показать, что $\exists i : L(g_i) \mid L(f)$. Распишем

$$h = (h_{11}g_1 + \dots + h_{1k_1}g_s) + \dots + (h_{s1}g_1 + \dots + h_{1k_s}g_s)$$

Рассмотрим $R_i^{h_{ij}(g_i)}(h_{ij}g_i) = h_{ij}g_i - h_{ij}g_i = 0$. Тогда $n(h_{ij}g_i) = 0$. Так как $L = K[x_1, \dots, x_n]$, справедливо $n(f) = N(h_{11}g_1) + \dots + N(h_{sk_s}g_s) = n(h_{11}g_1) + \dots + n(h_{sk_s}g_s) = 0$. Тогда найдется $R : R(f) = 0$. $R(f) = R(L(f)) + R(f - L(f))$. Так как $L(f)$ под действием оператора остается таким же, $R(L(f)) = L(f)$. Но $R(f - L(f))$ меньше $L(f)$, поэтому $R(L(f)) + R(f - L(f)) \neq 0$, противоречие. □

Пример. Возьмем идеал $I = (x_1^2 + x_2, x_1^2 + x_3) = (x_1^2 + x_2, x_2 - x_3)$. Проверим, является ли он базисом Гребнера. Рассмотрим $S(x_1^2 + x_2, x_2 - x_3) = x_2(x_1^2 + x_2) - x_1^2(x_2 - x_3) = x_2^2 + x_1^2x_3 \to x_2^2 - x_2x_3 \to 0$. Значит, является.

Алгоритм Бухбергера Начинаем с $\mathcal{F} = \{f_1, \dots, f_k\}$ — какой-то набор многочленов. Хотим получить базис Гребнера $G = \{f_1, \dots, f_k, f_{k+1}, \dots, f_n\}$ *того же самого идеала.*

Шаг 1 Упорядочим пары сначала по правой границе, затем по левой.

Шаг 2 Берем $(i, j) : S(f_1, f_2) \to N(S(f_1, f_2))$. Возможно 2 случая:

1. Если $N(S(f_1, f_2)) = 0$, то алгоритм заканчивается.
2. Иначе считаем $f_{k+1} = N(S(f_1, f_2))$. Перейдем к шагу 1 с набором $\{f_1, \dots, f_{k+1}\}$.

Факт 6. Если у многочленов взаимно простые старшие члены, то они редуцируются к 0.

Предложение 11. Алгоритм закончится за конечное число шагов и приведет к базису Гребнера.

Доказательство. От противного, пусть не останавливается. Пусть $f_1, \dots, f_k, f_{k+1}, \dots$. Но тогда мы знаем, что $\forall p > k : L(f_r) \nmid L(f_p)$ при $r < p$. Но получаем противоречие с леммой Диксона, поскольку тогда получаем бесконечно убывающую цепочку.

Теперь докажем, что идеал не изменится. Это очевидно, поскольку $f_{k+1} \in (f_1, \dots, f_k) \Rightarrow (f_1, \dots, f_k) = (f_1, \dots, f_{k+1})$.

И наконец покажем, почему мы получим базис Гребнера. Пусть $f_p = N(S(f_i, f_j))$ добавлен. Тогда $S(f_i, f_j) \to 0$. Действительно, $R_p^{L(f_p)}(N(S(f_i, f_j))) = f_p - f_p = 0$. Тогда по пункту 3 из критерия Бухбергера это базис Гребнера. □

Определение 63. *Базис Гребнера $\{g_1, \dots, g_s\}$ называется минимальным, если выполнено 3 условия:*

1. $\forall i = 1, \dots, s$ *старший коэф* g_i *не равен* 1.
2. $L(g_i) \nmid L(g_j)$ *при* $i \neq j$.
3. $\forall i = 1, \dots, s$ *любой не старший член* g_i *является G-нормальным.*

Утверждается, что из любого базиса Гребнера можно сделать минимальный. Старший коэффициент исправляется легко. Если $\exists i, j\ (i \neq j) : L(g_i) \mid L(g_j)$, то просто выбросим g_j. Идеал от этого не изменится $\Rightarrow$ базис Гребнера останется валидным. А для третьего пункта просто редуцируем нестаршие члены к нормальной форме.

Теорема 16. $\forall I \subseteq K[x_1, \dots, x_n]$ *минимальный базис Гребнера существует и единственен (считаем, что лексикографический порядок переменных фиксирован).*

Доказательство. Существование уже доказано (привели алгоритм). Докажем единственность. Пусть $G = \{g_1, \dots, g_s\}$, $H = \{h_1, \dots, h_k\}$ — два минимальных базиса Гребнера. Сначала покажем, что $s = k$ и с $L(g_i) = L(h_i)$ с точностью до перенумерации. По условию, $\forall i \exists j : L(g_j) \mid L(g_i)$. Также $\exists p : L(g_p) = L(g_i)$. Тогда $\forall i : L(g_p) \mid L(g_i)$. Но тогда $p = i$, следовательно можно поставить в соответствие $L(h_j) = L(g_i)$.

Теперь покажем, что они просто совпадают. Пусть не так, $\exists i : h_i \neq g_i$. Тогда $0 \neq h_i - g_i \Rightarrow L(h_i - g_j)$ это один из нестарших членов h_i или g_j. Но $h_i - g_j \in I$. По определению базиса Гребнера $L(g_t) \mid L(h_i - g_j)$. □

Применение базисов Гребнера

1. Проверка на принадлежность $f \in (f_1, \dots, f_k)$. Строим базис Гребнера $(f_1, \dots, f_k)$ и находим $N_G(f)$. Если $N_G(f) = 0$, то принадлежит, иначе нет.
2. Даны 2 идеала $I_1 = (f_1, \dots, f_k), I_2 = (h_1, \dots, h_s)$. Хотим проверить, совпадают ли они. Здесь нужно просто посчитать минимальные базисы Гребнера для I_1, I_2 и сравнить их. Можно также проверить, что $\forall i : f_i \in (h_1, \dots, h_s)$.