Лекция 3: Конечная порождённость идеалов в кольце многочленов

3.1 Мономиальные идеалы

Определение 3.1: Идеал $I \subset k[x_1, \dots, x_n]$ называется **мономиальным**, если он представляется в виде $I = \langle x^\alpha : \alpha \in A \rangle$, где A – некоторое подмножество в $\mathbb{Z}^n_{\geq 0}$.

Лемма 3.1: Пусть $I = \langle x^\alpha : \alpha \in A \rangle$ – мономиальный идеал. Тогда моном $x^\beta \in I \Leftrightarrow$ когда x^β делится на некоторый моном $x^\alpha \in I$.

Доказательство: Если x^β делится на $x^\alpha \in I$, то для некоторого x^γ выполняется $x^\beta = x^\gamma x^\alpha$. Поэтому моном $x^\beta \in I$.

Если $x^\beta \in I$, то он является комбинацией мономов $x^{\alpha(i)} \in I$ с полиномиальными коэффициентами h_i. Записав эти коэффициенты как линейные комбинации мономов и раскрыв скобки, мы получим, что x^β делится на какой-то из мономов $x^{\alpha(i)}$. ◀

Лемма 3.2: Пусть I – мономиальный идеал и $f \in k[x_1, \dots, x_n]$. Тогда следующие условия эквивалентны:

1) $f \in I$.
2) Каждый из составляющих f мономов лежит в I.
3) f является k-линейной комбинацией мономов из I

Доказательство: Нетривиальным является лишь утверждение $1) \Rightarrow 3)$, докажем его. Пусть $f \in I$, тогда $f = \sum_{i=1}^{\ell} h_i x^{\alpha(i)}$, где $h_i \in k[x_1, \dots, x_n]$. Записав h_i как линейные комбинации мономов, а затем умножив их на мономы $x^{\alpha(i)}$, мы получим каждый одночлен в произведениях лежит в идеале I. ◀

Следствие: Пусть $I, J \subset k[x_1, \dots, x_n]$ – мономиальные идеалы. Тогда $I = J$, если и только, если выполняется условие

$$(3.1) \qquad x^\alpha \in I \Leftrightarrow x^\alpha \in J.$$

Доказательство: Если $I = J$, то они, очевидно, содержат одни и те же мономы.
Обратно, если $f \in I$, то по 3) леммы 3.2 $f = \sum_{j=1}^{N} c_j x^{\alpha(j)}$, где $c_j \in k$ и $x^{\alpha(j)} \in I$. По условию (3.1) все $x^{\alpha(j)} \in J$, поэтому $f \in J$, т.е. $I \subset J$. Аналогично доказывается включение $J \subset I$. ◀

Теорема 3.1 (лемма Диксона): Пусть $I = \langle x^\alpha : \alpha \in A \rangle$ — мономиальный идеал. Тогда найдутся $\alpha(1), \dots, \alpha(s) \in A$, т.ч.

$$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle.$$

Иными словами, всякий мономиальный идеал конечно порождён мономами.

Доказательство: Индукцией по количеству переменных n. Пусть $I = \langle x_1^\alpha : \alpha \in A \rangle$, $A \subseteq \mathbb{Z}_{\geq 0}$, — мономиальный идеал в $k[x_1]$. Выберем наименьший элемент β во множестве A. Так как $\beta \leq \alpha$ для всех $\alpha \in A$, то моном x_1^β делит все мономы $x_1^\alpha \in I$. Следовательно, $I = \langle x_1^\beta \rangle$.

Предположим, что утверждение теоремы верно для $n-1$, где $n > 1$. Для удобства будем обозначать переменные через $x_1, \dots, x_{n-1}, y$, а мономы из $k[x_1, \dots, x_{n-1}, y]$ будем записывать в виде $x^\alpha y^m$, где $\alpha = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ и $m \in \mathbb{Z}_{\geq 0}$.

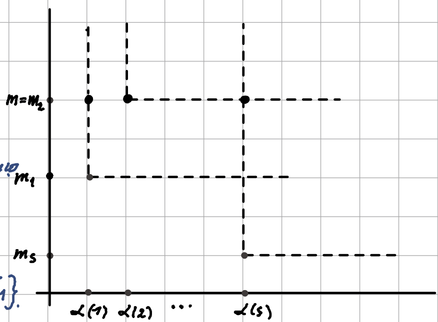
Пусть $I \subset k[x_1, \dots, x_{n-1}, y]$ — мономиальный идеал. Рассмотрим для I идеал $J \subset k[x_1, \dots, x_{n-1}]$, порождённый мономами x^α, т.ч. $x^\alpha y^m \in I$ для некоторого $m \geq 0$. По гипотезе индукции $J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. Тогда для каждого $i \in \{1, \dots, s\}$ выберем $m_i \geq 0$ — наименьшее среди чисел j, т.ч. $x^{\alpha(i)} y^j \in I$.

Через m обозначим максимум всех m_i.

Для $k \in \{0, \dots, m-1\}$ рассмотрим в $k[x_1, \dots, x_{n-1}]$ идеал J_k, порождённый мономами x^α, т.ч. $x^\alpha y^k \in I$. Каждый $J_k = \langle x^{\alpha^k(1)}, \dots, x^{\alpha^k(s_k)} \rangle$ по предположению.

Тогда идеал порождён мономами, входящими в конечный набор

$$\{x^{\alpha(1)} y^m, \dots, x^{\alpha(s)} y^m; x^{\alpha^k(1)} y^k, \dots, x^{\alpha^k(s_k)} y^k, k = \overline{0, m-1}\}.$$



Действительно, если $x^\alpha y^p \in I$, то при $p \geq m$ он делится на некоторый моном $x^{\alpha(i)} y^m$, а при $0 \leq p \leq m-1$ этот моном делится на некоторый моном $x^{\alpha^p(i)} y^p$. Тогда по лемме 3.1

$$x^\alpha y^p \in \langle x^{\alpha(1)} y^m, \dots, x^{\alpha(s)} y^m; x^{\alpha^k(1)} y^k, \dots, x^{\alpha^k(s_k)} y^k, k = \overline{0, m-1} \rangle.$$

Откуда по следствию из леммы 3.2 справедливо

$$I = \langle x^{\alpha(1)} y^m, \dots, x^{\alpha(s)} y^m; x^{\alpha^k(1)} y^k, \dots, x^{\alpha^k(s_k)} y^k, k = \overline{0, m-1} \rangle.$$

Следствие: Пусть $<$ — бинарное отношение на $\mathbb{Z}^n_{\geq 0}$, т.ч.

1) $(\mathbb{Z}^n_{\geq 0}, <)$ — линейно упорядоченное множество.
2) Если $\alpha < \beta$ и $\gamma \in \mathbb{Z}^n_{\geq 0}$, то $\alpha + \gamma < \beta + \gamma$.

Тогда $(\mathbb{Z}^n_{\geq 0}, <)$ — ВУМ $\Leftrightarrow$ когда $\alpha \geq 0$ для всех $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Доказательство: Пусть $(\mathbb{Z}^n_{\geq 0}, <)$ — ВУМ, а α_0 его наименьший элемент. Покажем, что $0 \leq \alpha_0$. Если $\alpha_0 < 0$, то с помощью 2) мы получим $2\alpha_0 < \alpha_0$, прибавив α_0 к обеим сторонам исходного неравенства. Это невозможно в силу выбора α_0.

Пусть $\alpha \geq 0$ для всех $\alpha \in \mathbb{Z}^n_{\geq 0}$, $A \subset \mathbb{Z}^n_{\geq 0}$ — непустое подмножество. Покажем, что в A есть наименьший элемент. Рассмотрим мономиальный идеал $I = \langle x^\alpha : \alpha \in A \rangle$. В силу леммы Диксона он может быть записан в виде $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$, где $\alpha(i) \in A$. Без ограничения общности можно считать, что $\alpha(1) < \alpha(2) < \dots < \alpha(s)$. Если $\alpha \in A$, то $x^\alpha \in \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. Тогда по лемме 31 моном x^α делится на некоторый $x^{\alpha(i)}$, т.е. $x^\alpha = x^\gamma \cdot x^{\alpha(i)}$, где $\gamma \geq 0$. Следовательно, по условию 2) мы имеем неравенство

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1),$$

которое означает, что $\alpha(1)$ — наименьший элемент в A. $\blacktriangleleft$

Определение 2.1': *Мономиальным порядком* $<$ на $k[x_1, \dots, x_n]$ называется линейный порядок на $\mathbb{Z}^n_{\geq 0}$ (или на множестве мономов), т.ч.

1) если $\alpha < \beta$ и $\gamma \in \mathbb{Z}^n_{\geq 0}$, то $\alpha + \gamma < \beta + \gamma$;
2) для всех $\alpha \in \mathbb{Z}^n_{\geq 0}$ выполняется $0 \leq \alpha$.

3.2 Базисы Грёбнера и теорема Гильберта о базисе

Определение 3.2: Пусть $I \subset k[x_1, \dots, x_n]$ — ненулевой идеал. *Идеалом старших членов* идеала I будем называть идеал, порождённый множеством

$$lt(I) := \{ cx^\alpha : \exists f \in I \ (lt f = cx^\alpha) \},$$

т.е. идеал $\langle lt(I) \rangle$.

Пример 3.1: Рассмотрим идеал $I = \langle \overbrace{x^3-2xy}^{f_1}, \overbrace{x^2y-2y^2+x}^{f_2} \rangle$, зафиксируем порядок deglex на $k[x,y]$. Сократим старшие члены образующих идеала I:

$$x(x^2y-2y^2+x) - y(x^3-2xy) = x^2.$$

Очевидно, что $x^2 \in \langle lt(I) \rangle$. Поскольку x^2 не делится ни на $lt f_1$, ни на $lt f_2$, моном $x^2 \notin \langle lt f_1, lt f_2 \rangle$. Таким образом, $\langle lt(I) \rangle \neq \langle lt f_1, lt f_2 \rangle$. ◀

Пример показывает, что идеал старших членов $\langle lt(I) \rangle$ идеала $I = \langle f_1, \dots, f_s \rangle$ может быть больше чем идеал $\langle lt f_1, \dots, lt f_s \rangle$.

Заметим, что поскольку мы работаем над полем $\langle lt(I) \rangle = \langle lm(I) \rangle$, где $lm(I) := \{ lm f : f \in I \}$, т.е. $\langle lt(I) \rangle$ - мономиальный идеал.

Предложение 3.1: Пусть $I \subset k[x_1, \dots, x_n]$ - ненулевой идеал. Тогда существуют $g_1, \dots, g_t \in I$, т.ч. $\langle lt(I) \rangle = \langle lt(g_1), \dots, lt(g_t) \rangle$.

Доказательство: Поскольку $\langle lm(I) \rangle$ - мономиальный идеал, то по лемме Диксона найдётся найдётся конечное число мономиальных образующих. По определению $\langle lm(I) \rangle$ эти образующие должны иметь вид $lm g_1, \dots, lm g_t$, где $g_1, \dots, g_t$ - некоторые многочлены из I. Таким образом,

$$\langle lm(I) \rangle = \langle lm g_1, \dots, lm g_t \rangle.$$

Очевидно, что $\langle lt(I) \rangle = \langle lt g_1, \dots, lt g_t \rangle$. ◀

Теорема 3.2 (Гильберта о базисе) Каждый идеал I в $k[x_1, \dots, x_n]$ конечно порождён, т.е. $I = \langle g_1, \dots, g_t \rangle$ для некоторых $g_1, \dots, g_t \in I$.

Доказательство: Нулевой идеал I порождён множеством $\{0\}$. Поэтому далее будем рассматривать ненулевой идеал $I \subset k[x_1, \dots, x_n]$. По предложению 3.1 найдутся $g_1, \dots, g_t \in I$, т.ч. $\langle lt I \rangle = \langle lt g_1, \dots, lt g_t \rangle$. Докажем, что $I = \langle g_1, \dots, g_t \rangle$.

Вложение $\langle g_1, \dots, g_t \rangle \subset I$ очевидно. Пусть $f \in I$, по теореме 2.1 (алгоритм деления) мы можем переписать f в виде

$$f = a_1 g_1 + \dots + a_t g_t + r, \tag{3.2}$$

где ни один моном в r не делится ни на один $lt g_1, \dots, lt g_t$. Покажем, что $r = 0$.

Предположим, что $r \neq 0$. Поскольку $r \in I$, то $\mathrm{lt}\, r \in \langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}\, g_1, \ldots, \mathrm{lt}\, g_t \rangle$. По лемме 3.1 $\mathrm{lt}\, r$ делится на какой-то $\mathrm{lt}\, g_i$, это противоречит тому, что r – остаток от деления f на $\{g_1, \ldots, g_t\}$. Следовательно, $r = 0$ и с учётом (3.2) $f \in \langle g_1, \ldots, g_t \rangle$, т.е. $I \subset \langle g_1, \ldots, g_t \rangle$ ◀

Определение 3.3: Зафиксируем мономиальный порядок на $k[x_1, \ldots, x_n]$. **Базисом Грёбнера** (**стандартным базисом**) идеала I называется конечное подмножество $G = \{g_1, \ldots, g_t\} \subset I$, т.ч.

(3.3) $$\langle \mathrm{lt}\, g_1, \ldots, \mathrm{lt}\, g_s \rangle = \langle \mathrm{lt}(I) \rangle$$

Следствие: Зафиксируем мономиальный порядок на $k[x_1, \ldots, x_n]$. Каждый ненулевой идеал $I \subset k[x_1, \ldots, x_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I порождает идеал I, т.е. является базисом идеала.

Доказательство: Конструкция набора $G = \{g_1, \ldots, g_t\}$, удовлетворяющего условию (3.3), приведена в доказательстве теоремы. Там же показано, что, если условие (3.3) выполняется, то $I = \langle g_1, \ldots, g_t \rangle$. ◀

Для идеала $I \subset k[x_1, \ldots, x_n]$ мы можем определить
$$\mathbb{V}(I) := \{ (a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \ \forall f \in I \}.$$

Предложение 3.2: Множество $\mathbb{V}(I)$ является аффинным многообразием. Если $I = \langle f_1, \ldots, f_s \rangle$, то $\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s)$.

Доказательство: По теореме Гильберта о базисе $I = \langle f_1, \ldots, f_s \rangle$ для некоторых $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Докажем, что $\mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_s)$. Прямое включение очевидно, поскольку $f_i \in I$, $i = 1, \ldots, s$. Возьмем $f \in I$, т.к. $I = \langle f_1, \ldots, f_s \rangle$ его можно записать в виде $f = h_1 f_1 + \ldots + h_s f_s$. Для точки $(a_1, \ldots, a_n) \in \mathbb{V}(f_1, \ldots, f_s)$ значение
$$f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n)\, f_i(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0.$$
Поэтому $\mathbb{V}(f_1, \ldots, f_s) \subset \mathbb{V}(I)$ ◀

Таким образом, аффинные многообразия определяются идеалами.

3.3 Нётеровы кольца

Определение 3.4: Кольцо R называется **нётеровым**, если любой идеал $I \subset R$ является конечно порождённым.

Предложение 3.3: Кольцо R нётерово $\Leftrightarrow$ когда выполняется **условие возрастающих цепочек** идеалов в R: если $I_1 \subset I_2 \subset \ldots \subset I_j$ — возрастающая цепочка идеалов I_j в R, то для достаточно больших j имеем $I_j = I_{j+1}$ (всякая непустая совокупность идеалов в R имеет максимальный элемент).

Доказательство: Пусть R нётерово. Рассмотрим $I_1 \subset I_2 \subset \ldots \subset I_j \subset \ldots$ — возрастающую цепочку идеалов в R. Объединение $I = \bigcup_i I_i$ является идеалом в R. Поскольку этот идеал конечно порождён, то все его образующие должны лежать в некотором I_j. Тогда $I_i = I$ для $i \geq j$.

Пусть выполняется условие возрастающих цепочек. Предположим, что некоторый идеал $I \subset R$ не является конечно порождённым. Тогда мы можем рассмотреть бесконечно возрастающую цепь

$$\langle f_1 \rangle \subset \langle f_1, f_2 \rangle \subset \langle f_1, f_2, f_3 \rangle \subset \ldots$$

Противоречие показывает, что R нётерово. ◀

Теорема 3.2' (Гильберта о базисе) Пусть R нётерово. Тогда кольцо многочленов $k[x]$ тоже является нётеровым.

Остаётся установить неравенство (2.4). Заметим, что каждое слагаемое в a_i имеет вид $\operatorname{lt} p^{(k)} / \operatorname{lt} f_i$. Начальное значение $p^{(0)} = f$, поэтому в силу только что доказанного, $\operatorname{lt} p^{(k)} < \operatorname{lt} f$ для всех k. Следовательно, для всех $i \in \{1, \ldots, s\}$

$$\operatorname{lt}(a_i f_i) = \operatorname{lt} a_i \operatorname{lt} f_i = \frac{\operatorname{lt} p^{(k_i)}}{\operatorname{lt} f_i} \cdot \operatorname{lt} f_i = \operatorname{lt} p^{k_i} < \operatorname{lt} f.$$

◀

Если в результате деления f на $\{f_1, \ldots, f_s\}$ остаток $r = 0$, то многочлен $f \in \langle f_1, \ldots, f_s \rangle$. Однако обратное неверно.

Пример 2.3: Пусть $f_1 = xy + 1$, $f_2 = y^2 - 1$ из $\mathbb{Q}[x, y]$ с lex: $x > y$. Поделив многочлен $f = xy^2 - x$ на (f_1, f_2), получим

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

Однако $xy^2 - x = x(y^2 - 1) \in \langle f_1, f_2 \rangle$.

◀