Лекция 2
Идеалы в кольце многочленов

В лекции 1 была рассмотрена конструкция "набор многочленов от n переменных" $\mapsto$ "множество точек в $\mathbb{K}^n$". При этом мы пришли к понятию алгебраического многообразия. Сейчас мы рассмотрим обратную конструкцию и придем к понятию идеала.

Одно и то же алгебраическое многообразие может быть задано разными наборами многочленов. Например, ось x в трехмерном пространстве можно задать как $V(y, z)$, а можно как $V(y + z, y - z)$. Ясно, что если многочлены f_1, ..., f_m обращаются в 0 в точках какого-то множества в пространстве $\mathbb{K}^n$, то любая комбинация, которую из них можно составить по формуле $g_1 f_1 + \ldots + g_m f_m$, где g_i — произволные многочлены, также будет обращаться в 0 в точках того же множества.

Определение. Идеал – это множество многочленов, замкнутое относительно взятия линейных комбинаций с произвольными полиномиальными коэффициентами. Иначе говоря, множество $F \subset \mathbb{K}[x_1, \ldots, x_n]$ называется идеалом, если для любых $f_1, ..., f_k \in F$ и для любых $g_1, ..., g_k \in \mathbb{K}[x_1, \ldots, x_n]$ выполняется свойство:

$$g_1 f_1 + ... + g_k f_k \in \mathbb{K}[x_1, \ldots, x_n].$$

Две конструкции идеала.

1. По набору многочленов: если даны несколько многочленов

$$a_1, \ldots, a_m \in \mathbb{K}[x_1, \ldots, x_n],$$

то можно определить идеал, ими порожденный. Этот идеал обозначается $\langle a_1, \ldots, a_m \rangle$ и состоит по определению из всех многочленов, представимых в виде линейных комбинаций $g_1 a_1 + ... + g_m a_m$, где g_1m ..., g_m —произвольные многочлены от $x_1, ..., x_n$. Набор многочленов $a_1, \ldots, a_m$ называется *системой образующих* или *базисом* рассматриваемого идеала.

2. По множеству точек в пространстве $\mathbb{K}^n$. Пусть $M \subset \mathbb{K}^n$ — произвольное множество. Обозначим через $I(M)$ совокупность всех многочленов, которые обращаются в ноль во всех точках множества M:

$$I(M) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(p) = 0 \ \forall p \in M\}.$$

Тогда $I(M)$ представляет собой идеал в кольце многочленов от n переменных.

Примеры.

1-1. $\langle x \rangle$ — идеал в кольце многочленов от одной переменной x, состоящий из всех многочленов вида xf, где f — произвольный многочлен. Очевидно, что это все многочлены без свободного члена.

1-2. Идеал $\langle x, y \rangle$ состоит из многочленов вида $xf+yg$. Это многочлены от двух переменных без свободного члена.

1-3. Идеал $\langle x^3, x^2y^2, y^3 \rangle$ состоит из всех многочленов вида $x^3f+x^2y^2g+y^3h$.

2-1. $I(\{0\})$ состоит из всех многочленов от одной переменной, которые обращаются в 0 в точке 0. Это все равно, что многочлены от x без свободного члена.

2-2. $I(\{(0,0)\})$ состоит из всех многочленов от двух переменных, значение которых в точке $(0,0)$ равно 0. Значит, речь идет о многочленах от x, y без свободного члена.

2-3. Пример 1-3 невозможно получить конструкцией 2.

Вывод: конструкция 1 сильнее, т.е. позволяет получить больше идеалов, чем конструкция 2. На самом деле, имеет место следующая теорема.

Теорема Гильберта о базисе. Любой идеал в кольце многочленов имеет вид $\langle f_1, \ldots, f_k \rangle$ для подходящего набора многочленов $f_1, \ldots, f_k$.

В чем практическое значение понятия идеала для элементарной алгебры? Оно помогает понять процесс извлечения следствий из системы уравнений с целью нахождения ее решений.

Пример. Рассмотрим систему уравнений

$$\begin{cases} x^2 + y^2 = 5, \\ xy = 2. \end{cases}$$

Пусть $I = \langle f_1, f_2 \rangle$, где $f_1 = x^2 + y^2 - 5$, $f_2 = xy - 2$. Тогда многочлен $f = y^2 f_1 - (xy + 2)f_2 = y^4 - 5y^2 + 4$ принадлежит идеалу I и, следовательно, уравнение $y^4 - 5y^2 + 4 = 0$ является следствием данной системы. В это уравнение входит только одна неизвестная, поэтому его легко решить. Подставляя найденные значения y в исходную систему, находим соответствующие значения x. При этом возникает вопрос: как найти такую комбинацию данных многочленов f_1, f_2, которая не зависит от x.

Ответ на этот вопрос дает понятие базиса Гребнера и алгоритм Бухбергера (см. ниже).

Теорема. Всякий идеал в кольце многочленов от одной переменной порожден каким-то *одним* многочленом.

Доказательство основано на алгоритме Евклида: пара многочленов $\{f, g\}$, где степень f больше или равна степени g, заменяется на пару $\{h, g\}$, где h — остаток от деления f на g; затем процесс итерируется.

Пример. $\langle x^4 - 1, x^6 - 1\rangle = \langle x^2 - 1\rangle$.

Задачи.

1. Найти многочлен f такой, что $\langle x^4 + 5x^2 - 4x - 2, x^3 + 2x - 3\rangle = \langle f\rangle$.

2. Существует ли такой многочлен f, что $\langle x^4 - 2, x^6 - 1\rangle = \langle f\rangle$?

3. Переход от параметрического уравнения к общему. Кривая на плоскости задана уравнениями $x = 2t/(t^2 + 1)$, $y = (t^2 - 1)/(t^2 + 1)$. Найти ее уравнение в виде $f(x, y) = 0$, где f — какой-то многочлен.

Домашнее задание.

1. Плоская кривая задана параметрически соотношениями $x = t^2 + 1, y = t^3 + 1$. Найдите ее уравнение в виде $f(x, y) = 0$.

2. Правда ли, что следующие два идеала совпадают: $\langle x^2, y^2, xy+x, xy+y\rangle = \langle x, y\rangle$?

3. Найдите многочлен $f(x)$ такой, что $\langle x^4 - 1, x^6 - 1\rangle = \langle f\rangle$.