Лекция 1

Пусть R – коммутативное кольцо. Напомним, что подмножество $I \subset R$ называется *идеалом*, если I – подгруппа по сложению и $\forall r \in R, i \in I$ выполнено $ri \in I$. Идеал I будем задавать множеством его порождающих: $I = (a_1, \ldots, a_k)$, если $I = \{\sum_{i=1}^{k} r_i a_i\}$. Если можно выбрать порождающие так, что $k = 1$, то идеал называется главным.

Важная задача состоит в том, чтобы по элементу $r \in R$ понять, лежит ли он в данном идеале, или нет.

Начнчм с примера.

Пример 1. $R = \mathbb{Z}$.

Кольцо $\mathbb{Z}$ евклидово. Из этого следует, что все идеалы кольца $\mathbb{Z}$ являются главными. Рассмотрим следующий алгоритм проверки вхождения элемента $b \in \mathbb{Z}$ в идеал $(a_1, \ldots, a_k)$.

Шаг 1 *Находим $d = НОД(a_1, \ldots, a_k)$. НОД находится по алгоритму Евклида. Тогда $(a_1, \ldots, a_k) = (d)$.*

ШАГ 2 *Делим b на d с остатком. Если остаток равен нулю, то $b \in I$, иначе $b \notin I$.*

Аналогичный алгоритм проверяет вхождение элемента в идеал для любого евклидова кольца, например для кольца $\mathbb{K}[x]$, где $\mathbb{K}$ – поле . (В таких кольцах корректно определено деление с остатком.) Наша цель – получить подобный алгоритм для кольца $\mathbb{K}[x_1, \ldots, x_n]$. Для этого мы определим аналог деления с остатком. "Делить"мы будем многочлен на систему многочленов, правда остаток будет не всегда однозначно определчн.

Напомним некоторые сведения о мономиальных порядках. Моном – это произведение $x_1^{l_1} \ldots x_n^{l_n}$. Мы хотим, чтобы про любые два различных монома можно было сказать, что либо один больше другого, либо второй больше первого. Кроме того мы хотим, чтобы порядок обладал следующими важными свойствами:

1) Антисимметричность. Если $M > N$, то не верно, что $N > M$.

2) Транзитивность. Если $M > N$ и $N > L$, то $M > L$.

3) Согласованность с умножением. Если $M > N$, то для любого монома L выполнено $ML > NL$.

4) Условие обрыва убывающих цепочек. Не существует бесконечной убывающей цепочки мономов.

Приведчм стандартные примеры мономиальных порядков, удовлетворяющих этим свойствам.

Пример 2. *Лексикографический порядок (***lex***). Мономы сравниваются по степени x_1. Если степень при x_1 у одного из мономов больше, то он больше. Если степени при x_1 одинаковы, то сравниваем степени у x_2 и т.д.*

Лексикографический порядок зависит от упорядочения переменных. Если упорядочить их по-другому, то получится другой порядок.

Единственное, что не очевидно, это то, что данный порядок удовлетворяет условию обрыва убывающих цепочек. Этот факт оставим в виде упражнения.

Пример 3. *Однородный лексикографический порядок (***deglex***). Мономы сравниваются по суммарной степени по всем паременным. Мономы с одинаковой суммарной степенью сравниваются лексикографически. Для этого порядка все аксиомы очевидны.*

Пусть фиксирован некоторый мономиальный порядок. Для дальнейшего можно считать, что это **lex**.

Пусть f – некоторый многочлен из $\mathbb{K}[x_1, \ldots, x_n]$. Старший член этого многочлена – это максимальный из его мономов с тем же коэффициентом, который у этого монома в многочлене f. Обозначаем его $LT(f)$.

Определение 1. Пусть $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Пусть некоторый член M многочлена f делится на $LT(g)$. *Элементарной редукцией $R(f, g, cM)$ многочлена f по многочлену g (относительно члена cM)* называется отображение $f \mapsto f - \frac{cM}{LT(g)}g$.

Элементарная редукция заменяет один член многочлена на сумму меньших членов.

Пример 4. *Пусть* $f = 2x_1^4x_2^3x_3^2 + 3x_1^3x_2^3x_3^3 + 4x_1^2x_2^3x_3^4$, $g = x_1^3x_2 + 3x_1x_2^2x_3$. *Тогда* $LT(g) = x_1^3x_2$. *Есть два варианта применить элементарную редукцию к* f, *так как*

$$\frac{2x_1^4x_2^3x_3^2}{x_1^3x_2} = 2x_1x_2^2x_3^2, \qquad \frac{3x_1^3x_2^3x_3^3}{x_1^3x_2} = 3x_2^2x_3^3 :$$

$$R(f, g, 2x_1^4x_2^3x_3^2) : f \mapsto f - 2x_1x_2^2x_3^2g = 3x_1^3x_2^3x_3^3 + 4x_1^2x_2^3x_3^4 - 6x_1^2x_2^4x_3^3,$$
$$R(f, g, 2x_1^4x_2^3x_3^2) : f \mapsto f - 3x_2^2x_3^3g = 2x_1^4x_2^3x_3^2 + 4x_1^2x_2^3x_3^4 - 9x_1x_2^4x_3^4.$$

Определение 2. Пусть $f, g_1, \ldots, g_k \in \mathbb{K}[x_1, \ldots, x_n]$. *Редукцией* f относительно системы $\{g_1, \ldots, g_k\}$ назовчм цепочку элементарных редукций по g_i.

Если к многочлену $\widehat{f}$ невозможно применить редукцию ни по какому g_i, то многочлен $\widehat{f}$ называется *нередуцируемым* относительно системы $\{g_1, \ldots, g_k\}$.

Пусть нередуцируемый многочлен r получен редукцией по системе $\{g_1, \ldots, g_k\}$ из многочлена f. Тогда r называется *остатком* f относительно системы $\{g_1, \ldots, g_k\}$.

Замечание 1. Остаток данного многочлена по данной системе не всегда определен однозначно.

Однако всегда можно гарантировать, что остаток существует.

Лемма 1. *Для любого f и любой системы $\{g_1, \ldots, g_k\}$ не существует бесконечной цепочки редукций f относительно $\{g_1, \ldots, g_k\}$.*

Доказательство. Старший член многочлена L_1 при элементарной редукции либо не меняется, либо уменьшается. Так как он не может уменьшаться бесконечно, с некоторых пор (с шага i_1) он не меняется. Начиная с шага i_1 будем следить за вторым по порядку членом L_2. Он либо не меняется, либо убывает. Найдчтся шаг $i_2 > i_1$, начиная с которого второй член не уменьшается и т.д. В итоге получаем бесконечно убывающую цепочку мономов: $L_1(i_1) > L_2(i_2) > L_3(i_3) > ...$ □

Определение 3. Система $\{g_1, \ldots, g_k\}$ называется *системой Гребнера.* если для любого f его остаток относительно данной системы однозначен (т.е. не зависит от последовательности элементарных редукций).

Система порождающих идеала называется *базисом Гребнера* (БГ), если она является системой Гребнера.

Алгоритм проверки принадлежности f идеалу будет состоять из двух шагов: первый шаг будет состоять из построения БГ данного идеала, а второй – из поиска остатка f относительно этого базиса. Если остаток 0, то f лежит в идеале. Иначе – не лежит.