ЛЕКЦИЯ 17

МНОГОЧЛЕНЫ ОДНОЙ И МНОГИХ ПЕРЕМЕННЫХ

АЛГОРИТМ ДЕЛЕНИЯ С ОСТАТКОМ

КОЛЬЦО МНОГОЧЛЕНОВ

Пусть R — коммутативное (и, как обычно, ассоциативное) кольцо с единицей 1, A — некоторое его подкольцо, содержащее 1.

Если $t \in R$, то наименьшее подкольцо в R, содержащее A и t, будет, очевидно, состоять из элементов

$$a(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n, \quad a_s \in A,\ n \in \mathbb{N}.$$

Мы обозначим его $A[t]$ и назовем кольцом, полученным из A присоединением элемента t, а выписанное выражение — многочленом от t с коэффициентами в A.

Теперь вспомним, что t — наугад взятый элемент кольца R, поэтому внешне различные выражения, записанные многочленами, могут на самом деле совпадать. Если, например, $A = \mathbb{Q}$, $t = \sqrt{2}$, то $t^2 = 2$, $t^3 = 2t$ — соотношения, которые никоим образом не вытекают из формальных правил.

Чтобы прийти к привычному понятию многочлена, необходимо освободиться от всех таких побочных соотношений, для чего под t следует понимать произвольный символ, не обязательно содержащийся в R.

Пусть теперь R — произвольное коммутативное кольцо с единицей. Построим новое кольцо S, элементами которого являются бесконечные упорядоченные последовательности

$$a = (a_0, a_1, a_2, \dots), \quad a_i \in R,$$

такие, что все a_i, кроме конечного числа, равны нулю.

Определим на множестве S операции сложения и умножения, полагая

$$a+b = (a_0, a_1, a_2, \dots)+(b_0, b_1, b_2, \dots) = (a_0+b_0, a_1+b_1, a_2+b_2, \dots)$$

и

$$a \cdot b = c = (c_0, c_1, c_2, \dots),$$

где

$$c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, 1, 2, \dots$$

Ясно, что в результате сложения и умножения получается снова последовательности элементов кольца с конечным числом отличных от нуля членов.

Проверка всех аксиом кольца, кроме, разве что, аксиомы ассоциативности сложения, очевидна.

Действительно, поскольку сложение двух элементов из S сводится к сложению конечного числа элементов из кольца R, то структура $(S, +)$ является коммутативной группой с нулевым элементом $(0, 0, 0, \dots)$.

Далее, коммутативность умножения следует непосредственно из симметричности выражения коэффициентов c_k через a_i и b_j.

Также выражение произведения и суммы показывают, что в S выполнен закон дистрибутивности.

Теперь покажем, что выполнена ассоциативность умножения.

Пусть

$$a = (a_0, a_1, a_2, \dots), \quad b = (b_0, b_1, b_2, \dots), \quad c = (c_0, c_1, c_2, \dots)$$

— три произвольных элемента множества S.

Тогда

$$ab = d = (d_0, d_1, d_2, \dots),$$

где

$$d_l = \sum_{i+j=l} a_i b_j, \quad l = 0, 1, 2, \dots,$$

а

$$(ab)c = dc = e = (e_0, e_1, e_2, \dots),$$

где

$$e_s = \sum_{l+k=s} d_l c_k = \sum_{l+k=s} \left(\sum_{i+j=l} a_i b_j \right) c_k = \sum_{i+j+k=s} a_i b_j c_k.$$

Смотря на это выражение, ясно, что оно никак не зависит от расстановки скобок, поэтому операция ассоциативна.

Итак, S — ассоциативное коммутативное кольцо с единицей $(1, 0, 0, \dots)$.

Последовательности $(a, 0, 0, \dots)$ складываются и умножаются как элементы кольца R.

Это позволяет отождествить такие последовательности с элементами из R, то есть положить

$$a := (a, 0, 0, \dots) \text{ для всех } a \in R.$$

Тем самым R становится полкольцом кольца S.

Обозначим, далее, $(0, 1, 0, 0, \dots)$ через X и назовем X *переменной* (или *неизвестной*) над R.

Используя введенную на S операцию умножения, находим, что

$$\begin{aligned} X &= (0, 1, 0, 0, \dots), \\ X^2 &= (0, 0, 1, 0, \dots), \\ &\dots\dots\dots\dots\dots\dots \\ X^n &= (0, 0, \dots, 1, 0, \dots). \end{aligned}$$

Кроме того, легко убедиться, что

$$(0, 0, \dots, 0, a, 0, \dots) = aX^n = X^n a.$$

Итак, если a_n — последний отличный от нуля член последовательности $a = (a_0, a_1, \dots, a_n, 0, 0, \dots)$, то в новых обозначениях

$$\begin{aligned} a = (a_0, \dots, a_{n-1}, 0, 0, \dots) + a_n X^n = \\ = (a_0, \dots, a_{n-2}, 0, 0, \dots) + a_{n-1} X^{n-1} + a_n X^n = \\ = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n. \end{aligned}$$

Такое представление элемента a однозначно.

Определение 1. Введенное выше кольцо S обозначается через $R[X]$ и называется *кольцом многочленов над* R от одной переменной X, а его элементы — многочленами (или полиномами).

Элементы a_i называют *коэффициентами* многочлена. Многочлен f — нулевой, если все его коэффициенты — нули. Коэффициент многочлена при нулевой степени называется *свободным членом*. Если $a_n \neq 0$, то его называют старшим коэффициентом, а n — степенью многочлена, пишут $n = \deg f$. Нулевому многочлену приписывается степень $-\infty$.

Непосредственно из определения операций сложения и умножения в $R[X]$ следует, что для любых двух многочленов

$$f = a_0 + a_1X + \dots a_nX^n \text{ и } g = b_0 + b_1X + \cdots + b_mX^m$$

степеней m и n соответственно имеют место неравенства

$$\deg(f+g) \leqslant \max(\deg f, \deg g), \quad \deg(fg) \leqslant \deg f + \deg g.$$

Второе из неравенств а самом деле заменяется равенством

$$\deg(fg) = \deg f + \deg g$$

всякий раз, когда произведение a_nb_m старших коэффициентов многочленов f и g отлично от нуля, поскольку

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + (a_nb_m)X^{n+m}.$$

Это значит, что верна

Теорема 1. *Если R — целостное кольцо, то и кольцо $R[X]$ является целостным.*

МНОГОЧЛЕНЫ МНОГИХ ПЕРЕМЕННЫХ

Если в ситуации $R \subset S$ взять произвольные n элементов $t_1, \ldots, t_n \in S$ и рассмотреть S как пересечение всех подколец, содержащих R и все $t_1, \ldots, t_n$, то мы получим кольцо $R[t_1, \ldots, t_n]$.

Теперь введем абстрактное кольцо многочленов от n переменных.

Делается это очень просто.

Вспомним, что конструкция кольца $S = R[X]$ включала произвольное коммутативное кольцо R с единицей. Мы можем теперь заменить в нашей конструкции кольцо R на S и построить кольцо $T = S[Y]$, где Y — новая независимая переменная, играющая по отношению к S ту же роль, что и X по отношению к R.

Элементы из T однозначно записываются в виде

$$\sum s_j Y^j, \quad s_j \in S,$$

причем S отождествляется с подкольцом в T, а именно с множеством элементов

$$sY^0 = s \cdot 1.$$

Так как в свою очередь

$$s_j = \sum r_{ij} X^i$$

— однозначная запись элементов $s_j \in S$, то любой элемент в T имеет вид

$$\sum_{i=0}^{k} \sum_{j=0}^{l} r_{ij} X^i Y^j, \quad r_{ij} \in R,$$

причем подразумевается (по смыслу конструкции), что r_{ij} перестановочны с X и Y, а X и Y перестановочны друг с другом.

Кольцо T называется кольцом многочленов над R от двух независимых переменных X и Y.

Повторив достаточное число раз эту конструкцию, мы получим кольцо

$$R[X_1, \ldots, X_n]$$

многочленов (полиномов) над R от n независимых переменных (или неизвестных) $X_1, \ldots, X_n$.

Набор $(i_1, \ldots, i_n) \in (\mathbb{N} \cup \{0\})^n$ из n целых неотрицательных чисел $i_1, \ldots, i_n$ условимся сокращенно обозначать символом (i).

Тогда любой элемент запишется в виде

$$f = \sum_{(i)} a_{(i)} X^{(i)}, \quad a_{(i)} \in R,$$

где

$$X^{(i)} = X_1^{i_1} \ldots X_n^{i_n}$$

— одночлен (или моном), так что f — линейная комбинация одночленов с коэффициентами из R.

В соответствии с определением многочленов все коэффициенты $a_{(i)}$, за исключением конечного числа, равны нулю.

Единственность записи непосредственно вытекает из следующего утверждения:

Предложение 1. *Многочлен f от многих переменных равен нулю тогда и только тогда, когда равны нулю все его коэффициенты $a_{i_1 \dots i_n}$.*

Доказательство. При $n = 1$ это уже отмечалось в ходе построения кольца $R[X]$, а при $n > 1$ проще всего использовать индукцию по n.

Именно, мы можем записать

$$f = \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} = \sum_{i_n} b_{i_n} X_n^{i_n},$$

где

$$b_{i_n} = \sum_{i_1, \dots, i_{n-1}} a_{i_1 \dots i_{n-1} i_n} X_1^{i_1} \dots X_{n-1}^{i_{n-1}}$$

— многочлены от меньшего числа переменных.

Утверждение для $n = 1$ и предположение индукции показывают, что

$$f = 0 \Longleftrightarrow \forall i_n \; b_{i_n} = 0 \Longleftrightarrow \forall (i_1, \dots, i_n) \; a_{i_1, \dots, i_{n-1}, i_n} = 0.$$

□

Теперь естественно считать два многочлена

$$f, g \in R[X_1, \dots, X_n]$$

равными,если совпадают их коэффициенты при одинаковых одночленах.

Под степенью многочлена f относительно X_k понимается наибольшее целое число, обозначаемое $\deg_k f$, которое встречается в качестве показателя при X_k в $a_{(i)}X^{(i)}$ с $a_{(i)} \neq 0$.

Например, многочлен

$$1 + X + XY^3 + X^2Y^2$$

имеет степень два относительно X и степень три относительно Y.

Целое число $i_1 + \cdots + i_n$ называется полной степенью одночлена

$$X_1^{i_1} \dots X_n^{i_n}.$$

Степенью $\deg f$ (или полной степенью) многочлена f будет максимальная из полных степеней его одночленов.

Полагаем $\deg 0 = -\infty$.

О старшем по степени члене многочлена f не имеет смысла говорить, потому что таких одночленов может быть несколько.

На кольцо $R[X_1, \dots, X_n]$ переносятся многие результаты, полученные нами на прошлой лекции для $R[X]$.

Например, очевидна теперь

Теорема 2. *Если R — целостное кольцо, то и кольцо $R[X_1, \dots, X_n]$ является целостным.*

В частности, кольцо многочленов от n переменных над полем F целостно.

Полезным уточнением предыдущей теоремы служит

Теорема 3. *Пусть f и g — произвольные многочлены от n переменных над целостным кольцом R. Тогда*

$$\deg(fg) = \deg f + \deg g.$$

Доказательство. Назовем однородным многочленом степени m многочлен $h(X_1, \ldots, X_n)$, все одночлены которого имеют одну и ту же полную степень m.

Объединяя вместе все входящие в f одночлены одной и той же степени, мы однозначно представим многочлен

$$f = \sum a_{(i)} X^{(i)}$$

в виде суммы нескольких однородных многочленов различных степеней

$$f = f_0 + f_1 + \cdots + f_k, \quad k = \deg f.$$

Если теперь

$$g = g_0 + g_1 + \cdots + g_l, \quad l = \deg g,$$

то, очевидно,

$$fg = (f_0 g_0) + (f_0 g_1 + f_1 g_0) + \cdots + f_k g_l,$$

откуда $\deg f \leqslant k + l$.

Условимся располагать одночлены любого нашего многочлена *лексикографически* (по принципу построения словаря), то есть таким образом, чтобы одночлен

$$u = a X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$$

предшествовал одночлену

$$b X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}$$

(или был больше одночлена v) в точности тогда, когда последовательность

$$i_1 - j_1, i_2 - j_2, \ldots, i_n - j_n$$

имеет вид

$$0, 0, \ldots, 0, t, \ldots, \text{ где } t > 0.$$

Справа от t могут стоят и отрицательные разности $i_1 - j_1$.

Одночлен, входящий в f и занимающий первое место при лексикографическом упорядочении, называется *высшим членом* многочлена f. Обозначим его $HM(f)$ (Highest Member).

Лемма 1. *Высшим членом произведения*

$$h = h_1 h_2 \ldots h_r$$

является произведение высших членов сомножителей

$$h_1, h_2, \ldots, h_r.$$

Доказательство. Действительно, при $n = 1$ утверждение верно, а если

$$h = h(X_1, X_2, \ldots, X_n) = \\ = g_0(X_2, \ldots, X_n)X_1^s + g_1(X_2, \ldots, X_n)X_1^{s-1} + \ldots,$$

то высший член многочлена h равен $X_1^s \cdot HM(g_0)$.

Разложим теперь по степеням каждый из сомножителей h_i, получив

$$HM(h_i) = X_1^{s_i} \cdot HM(g_i^{(0)}).$$

Понятно, что коэффициент $g_0(X_2, \ldots, X_n)$ получается как произведение соответствующих коэффициентов

$$g_0^{(1)}(X_2, \ldots, X_n), \ldots, g_0^{(r)}(X_2, \ldots, X_n),$$

поэтому наше утверждение получается по индукции по n. □

Таким образом, рассматриваемый нами $f_k g_l$ имеет степень $k+l$, то есть имеет место равенство. □

АЛГОРИТМ ДЕЛЕНИЯ С ОСТАТКОМ

Оказывается, что в кольце многочленов над целостным кольцом имеет место алгоритм деления с остатком, похожий на этот же алгоритм для целых чисел.

Теорема 4. *Пусть R — целостное кольцо и g — многочлен в $R[X]$ со страшим коэффициентом, обратимым в R.*

Тогда каждому многочлену $f \in R[X]$ сопоставляется одна и только одна пара многочленов $q, r \in R[X]$, для которых

$$f = qg + r, \quad \deg r < \deg g.$$

Доказательство. Пусть

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_n,$$
$$g = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$

где $a_0b_0 \neq$ и b_0 обратим.

Применим индукцию по n.

Если $n = 0$ и $m = \deg g > \deg f = 0$, то положим $q = 0$, $r = f$, а если $n = m = 0$, то $r = 0$, $q = a_0b_0^{-1}$.

Допустим, что теорема доказана для всех многочленов степени $< n$.

Без ограничения общности считаем $m \leqslant n$, так как в противном случае возьмем $q = 0$, $r = f$.

Раз это так, то

$$f = a_0b_0^{-1}X^{n-m} \cdot g + \overline{f},$$

где $\deg \overline{f} < n$.

По индукции мы можем найти $\overline{q}$ и r, для которых

$$\overline{f} = \overline{q}g + r,$$

причем $\deg r < m$.

Положив

$$q = a_0 b_0^{-1} X^{n-m} + \overline{q},$$

мы придем к паре многочленов с нужными свойствами.

Обращаясь к единственности частного q и остатка r, предположим, что

$$qg + r = f = q'g + r'.$$

Тогда

$$(q' - q)g = r - r'.$$

По теореме о степени произведения многочленов имеем

$$\deg(r - r') = \deg(q - q) + \deg g,$$

что в наших условиях возможно только при $r' = r$ и $q' = q$.

Наконец, приведенные рассуждения показывают, что коэффициенты частного q и остатка r принадлежат тому же целостному кольцу R, то есть

$$f, g \in R[X] \Longrightarrow q, r \in R[X].$$

□