ЛЕКЦИЯ 17

КОЛЬЦО МНОГОЧЛЕНОВ И ЕГО СВОЙСТВА

АЛГОРИТМ ДЕЛЕНИЯ С ОСТАТКОМ

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА ДЕЛИМОСТИ

ЕВКЛИДОВЫ КОЛЬЦА И АЛГОРИТМ ЕВКЛИДА

КОЛЬЦО МНОГОЧЛЕНОВ

ОПРЕДЕЛЕНИЕ 1. Для коммутативного кольца с единицей R кольцо S, состоящее из формальных сумм

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n, \text{ где } a_0, \ldots, a_n \in R, n \geqslant 0,$$

сложение задано правилом

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i,$$

а умножение — правилом

$$\sum_{i=0}^{n} a_ix^i \cdot \sum_{j=0}^{m} b_jx^j = \sum_{k=0}^{n+m} \sum_{l=0}^{k} a_lb_{k-l}x^k,$$

обозначается через $R[x]$ и называется *кольцом многочленов над* R от одной переменной x, а его элементы — многочленами (или полиномами).

Очевидно, что это коммутативное ассоциативное кольцо с единицей.

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

$$f = a_0 + a_1x + \ldots a_nx^n \text{ и } g = b_0 + b_1x + \cdots + b_mx^m$$

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 $a_n b_m$ старших коэффициентов многочленов f и g отлично от нуля, поскольку

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + (a_n b_m)x^{n+m}.$$

Это значит, что верна

Теорема 1. *Если R — целостное (без делителей нуля) кольцо, то и кольцо $R[x]$ является целостным.*

МНОГОЧЛЕНЫ МНОГИХ ПЕРЕМЕННЫХ

Теперь введем кольцо многочленов от n переменных.

Заметим, 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

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

□

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА ДЕЛИМОСТИ

Нас интересует кольцо $\mathbb{F}[x]$ многочленов над полем.

Начнем с произвольного целостного кольца R. Обратимые элементы в R называются делителями единицы.

Совершенно очевидно, что многочлен $f \in R[x]$ обратим тогда и только тогда, когда $\deg f = 0$ и $f = f_0$ — обратимый элемент кольца R.

Говорят, что элемент $b \in R$ *делится* на $a \in R$ (или b *кратен* a), если существует такой элемент $c \in R$, что $b = ac$ (это обозначается $a|b$).

Если $a|b$ и $b|a$, то a и b называются *ассоциированными* элементами. Тогда $b = ua$, где u — обратимый элемент.

В силу замечания, которое мы сделали выше, ассоциированность многочленов f и g означает, что они отличаются лишь обратимым множителем из R.

Элемент $p \in R$ называется *простым* (или *неразложимым*), если p необратим и его нельзя представить в виде $p = ab$, где a, b — необратимые элементы.

В поле $\mathbb{F}$ каждый ненулевой элемент обратим, поэтому там нет простых элементов.

Простой элемент кольца $R[x]$ называется обычно *неприводимым многочленом.*

Отметим следующие основные свойства отношения делимости в целостном кольце R:

(1) *Если* $a|b$, $b|c$, *то* $a|c$.

Действительно, мы имеем $b = ab'$, $c = bc'$, где $b', c' \in R$. Поэтому $c = (ab')c' = a(b'c')$.

(2) *Если* $c|a$, $c|b$, *то* $c|(a \pm b)$.

В самом деле, по условию $a = ca'$, $b = cb'$ для некоторых $a', b' \in R$, и ввиду дистрибутивности $a \pm b = c(a' \pm b')$.

(3) *Если* $a|b$, *то* $a|bc$.

Ясно, что $b = ab' \Longrightarrow bc = (ab')c = a(b'c)$.

Комбинируя (2) и (3), получаем

(4) *Если каждый из элементов* $b_1, b_2, \ldots, b_m \in R$ *делится на* $a \in R$, *то на* a *будет делиться также и элемент*

$$b_1c_1 + b_2c_2 + \cdots + b_mc_m,$$

где $c_1, c_2, \ldots, c_m$ — *произвольные элементы кольца.*

Определение 2. Говорят, что целостное кольцо R — *кольцо с однозначным разложением на простые множители* (или *факториальное кольцо*), если любой элемент $a \neq 0$ из R можно представить в виде

$$a = up_1p_2 \dots p_r,$$

где u — обратимый элемент, а $p_1, \dots, p_r$ — простые элементы (не обязательно попарно различные), причем из существования другого такого разложения

$$a = vq_1q_2 \dots q_s$$

следует, что $r = s$ и при надлежащей нумерации элементов p_i и q_j будет

$$q_1 = u_1p_1, \dots, q_r = u_rp_r,$$

где $u_1, \dots, u_r$ — обратимые элементы.

Мы допускаем, что $r = 0$, то есть обратимые элементы тоже раскладываются на простые множители.

Ясно, что если p — простой, u — обратимый, то up — тоже простой элемент.

В кольце $\mathbb{Z}$ с обратимыми элементами 1 и -1 отношение порядка дает возможность выделить положительное простое число p из двух возможных $\pm p$.

В кольце $\mathbb{F}[x]$ принято рассматривать нормализованные многочлены (с коэффициентом при старшей степени, равным единице).

Справедлива следующая общая

Теорема 5. *Пусть R — произвольное целостное кольцо с разложением на простые множители.*

Однозначность разложения в R имеет место тогда и только тогда, когда любой простой элемент $p \in R$, делящий произведение $ab \in R$, делит по крайней мере один из множителей a, b.

Доказательство. Пусть R факториально, и пусть $ab = pc$. Если

$$a = \prod a_i, \quad b = \prod b_j, \quad c = \prod c_k$$

— разложения a, b, c на простые множители, то из равенства

$$\prod a_i \times \prod b_j = p \prod c_k$$

следует, что элемент p ассоциирован с одним из a_i или b_j, то есть p делит a или b.

Обратно, установим однозначность разложения в R, где

$$p|ab \Longrightarrow p|a \text{ или } p|b.$$

Рассуждая по индукции, допустим, что разложение всех элементов из R с числом $\leqslant n$ простых множителей единственно (конечно, с точностью до порядка множителей и их ассоциированности).

Докажем теперь это для любого элемента $a \neq 0$, который может быть разложен на $n+1$ простых множителей. Именно, пусть

$$a = \prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} r_j$$

— два разложения элемента a с $m \geqslant n$.

Условие теоремы, примененное к $p = p_{n+1}$, дает нам, что p_{n+1} должен делить один из элементов $r_1, \ldots, r_{m+1}$.

Без ограничения общности (ибо это вопрос нумерации) считаем, что

$$p_{n+1} | r_{m+1}.$$

Но r_{m+1} — простой элемент, поэтому

$$r_{m+1} = u p_{n+1},$$

где u — обратимый элемент.

Опираясь на закон сокращения в R, получаем равенство

$$\prod_{i=1}^{n} p_i = u \prod_{j=1}^{m} r_j.$$

В левой части его стоит произведение n простых множителей. По предположению индукции $m = n$ и оба разложения отличаются лишь порядком простых элементов, снабженных, возможно, какими-то обратимыми множителями. $\square$

В произвольном целостном кольце R элемент $a \neq 0$ вообще не обязан допускать разложения на простые множители. Что более интересно, имеются целостные кольца, в которых разложение на простые множители хотя и возможно, но не является однозначным.

Пример 1. Рассмотрим поле $\mathbb{Q}[\sqrt{-5}]$, а в нем целостное кольцо

$$\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Норма

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

каждого отличного от нуля элемента $\alpha \in R$ — целое положительное число. Если α обратим в R, то

$$(N(\alpha))^{-1} = N(\alpha^{-1}) \in \mathbb{Z},$$

откуда $N(\alpha) = 1$. Это возможно лишь при $b = 0$, $a = \pm 1$.

Таким образом, в R обратимыми элементами, как и в $\mathbb{Z}$, являются только ± 1.

Если

$$\alpha = \varepsilon\alpha_1\alpha_2 \dots \alpha_r \neq 0, \quad \varepsilon = \pm 1,$$

то

$$N(\alpha) = N(\alpha_1) \dots N(\alpha_r).$$

Так как $1 < N(\alpha_i) \in \mathbb{N}$, то при заданном α число множителей r не может неограниченно расти.

Значит, разложение на простые множители в R возможно.

Вместе с тем число 9 (да и не только оно) допускает два существенно различных разложения на простые множители:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Неассоциированность элементов 3 и $2 \pm \sqrt{-5}$ очевидна.

Далее,

$$N(3) = N(2 \pm \sqrt{-5}) = 9.$$

Поэтому из разложения $\alpha = \alpha_1\alpha_2$ для $\alpha = 3$ или $2 \pm \sqrt{-5}$ с необратимыми α_1, α_2 следовало бы $9 = N(\alpha) = N(\alpha_1)N(\alpha_2)$, откуда $N(\alpha_i) = 3$ при $i = 1, 2$. Но это невозможно, так как уравнение $x^2 + 5y^2 = 3$ в целых числах неразрешимо. Отсюда следует простота элементов 3 и $2 \pm \sqrt{-5}$.

Наибольшим делителем НОД(a, b) двух элементов $a, b \in R$ целостного кольца R называется такой элемент d этого кольца, который удовлетворяет двум свойствам:

(1) $d|a, d|b$;

(2) Если $d'|a, d'|b$, то $d'|d$.

Очевидно что наибольший общий делитель двух элементов (если он существует) определен с точностью до ассоциированности.

Аналогично, наибольшим общим кратным НОК(a, b) двух элементов $a, b \in R$ называется такой элемент $c \in R$, что

(1) $a|c, b|c$;

(2) Если $a|c', b|c'$, то $c|c'$.

Аналогично, наименьше общее кратное также определено с точностью до ассоциированности.

Определение 3. Элементы a, b целостного кольца, в котором существует разложение на множители, называются взаимно простыми, если все их общие делители обратимы.

ЕВКЛИДОВЫ КОЛЬЦА И АЛГОРИТМ ЕВКЛИДА

Алгоритм деления с остатком в $\mathbb{Z}$ и $\mathbb{F}[X]$ делает естественным рассмотрение целостного кольца R, в котором каждому элементу $a \neq 0$ поставлено в соответствие неотрицательное целое число $\delta(a)$, то есть определено отображение

$$\delta : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

так, что при этом выполняются условия:

(1) $\delta(ab) \geqslant \delta(a)$ для всех $a, b \neq 0$ из R;

(2) каковы бы ни были $a, b \in R$, $b \neq 0$, найдутся $q, r \in R$ такие, что

$$a = bq + r, \quad \delta(r) < \delta(q) \text{ или } r = 0.$$

Целостное кольцо R с этими свойствами называют *евклидовым кольцом*. Полагая $\delta(a) = |a|$ для $a \in \mathbb{Z}$ и $\delta(a) = \deg a$ для $a = a(X) \in F[X]$, мы приходим к выводу, что $\mathbb{Z}$ и $\mathbb{F}[X]$ — евклидовы кольца.

В евклидовых кольцах существует способ нахождения НОД(a, b), называемый *алгоритмом последовательного деления* или *алгоритмом Евклида* и заключающийся в следующем.

Пусть даны ненулевые элементы a, b евклидова кольца R.

Применяя достаточно большое (но конечное) число раз правило (2), мы поулчим систему равенств с последним нулевым остатком:

$$\begin{aligned}
a &= q_1 b + r_1, & \delta(r_1) &< \delta(b),\\
b &= q_2 r_1 + r_2, & \delta(r_2) &< \delta(r_1),\\
r_1 &= q_3 r_2 + r_3, & \delta(r_3) &< \delta(r_2),\\
&\ldots\ldots\ldots\ldots & &\ldots\ldots\ldots\\
r_{k-2} &= q_k r_{k-1} + r_k, & \delta(r_k) &< \delta(r_{k-1}),\\
r_{k-1} &= q_{k+1} r_k, & r_{k+1} &= 0.
\end{aligned}$$

Это действительно так, поскольку строго убывающая цепочка неотрицательных целых чисел

$$\delta(b) > \delta(r_1) > \delta(r_2) > \ldots$$

должна оборваться, а обрыв может произойти только за счет обращения в нуль одного из остатков.

Утверждается, что последний отличный от нуля остаток r_k является как раз наибольшим общим делителем элементов a и b.

Доказательство. Действительно, по условию $r_k | r_{k-1}$. Двигаясь в данной системе снизу сверх, получим цепочку

$$r_k | r_{k-1}, \quad r_k | r_{k-2}, \ldots, r_k | r_2, \quad r_k | r_1,$$

и, наконец,

$$r_k | b, \quad r_k | a.$$

Значит, r_k — общий делитель элементов a и b.

Обратно, пусть c — некоторый общий делитель элементов a и b. Будем теперь двигаться по нашем системе в прямом направлении. Если c делит a и b, то делит и r_1. Если c делит b и r_1, то делит и r_2. Двигаясь так дальше, получаем, что c делит r_k, что и требовалось.

Значит,

$$r_k = \text{НОД}(a, b).$$

□

Заметим теперь, что каждый остаток r_i в системе выражется в виде линейной комбинации с коэффициентами из R от двух предыдущих остатков r_{i-1} и r_{i-2}. При этом r_1 выражается через a и b, а r_2 выражается через b и r_1, тем самым снова выражаясь через a и b. Последовательная подстановка в r_i выражений r_{i-1} и r_{i-2} через a и b даст нам при $i = k$ выражение

$$r_k = au + bv$$

с какими-то элементами $u, v \in R$.