ЛЕКЦИЯ 20

КОРНИ МНОГОЧЛЕНОВ, ТЕОРЕМА БЕЗУ

ДИФФЕРЕНЦИРОВАНИЯ МНОГОЧЛЕНОВ

ФОРМУЛЫ ВИЕТА

КОРНИ МНОГОЧЛЕНОВ

Займемся тем, ради чего в прошлом изучали алгебру, — корнями многочленов. Дело в том, что многие задачи математики в конечном счете сводятся к вычислению отдельных корней конкретных многочленов или к качественному описанию их совокупности.

Пусть коммутативное кольцо R с единицей содержится в целостном кольце S.

Определение 1. Элемент $c \in S$ называется *корнем* (или *нулем*) *многочлена* $f \in R[X]$, если $f(c) = 0$.

Говорят также, что c — корень уравнения $f(x) = 0$.

Необходимость рассмотрения колец, содержащих кольцо R собственным образом, станет понятной, если вспомнить, что многочлен $f(X) = X^2 + 1$ не имеет корней над полем $\mathbb{R}$, но при этом для $i \in \mathbb{C}$ имеет место $f(i) = 0$.

При этом сначала мы рассмотрим случай $S = R$.

Теорема 1 (теорема Безу)**.** *Элемент $c \in R$ является корнем многочлена $f \in R[X]$ тогда и только тогда, когда многочлен $X - c$ делит f в кольце $R[X]$.*

Доказательство. Эта теорема — часть более общего утверждения, которое мы могли бы доказать давно. А именно, алгоритм деления с остатком гласит, что

$$f(X) = (X - c)q(X) + r(X), \text{ где } \deg r(X) < \deg(X - c) = 1.$$

Значит, $r(X)$ — константа.

Подставим вместо X константу c:

$$f(c) = r(c),$$

то есть $r(X)$ — это константа c.

Таким образом, всегда

$$f(X) = (X - c)q(X) + f(c).$$

В частности,

$$f(c) = 0 \Longleftrightarrow f(X) = (X - c)q(X).$$

□

Деление многочлена $f(X)$ с коэффициентами в целостном кольце R на линейный многочлен $X - c$ удобно осуществлять по так называемой *схеме Горнера*, более простой, чем общий алгоритм деления с остатком.

Именно, пусть

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n, \quad a_i \in R.$$

По формуле, полученной в доказательстве теоремы Безу,

$$q(X) = b_0X^{n-1} + b_1X^{n-2} + \cdots + b_{n-1}, \quad b_j \in R.$$

Подставим теперь эти выражения в формулу

$$f(X) = (X - c)q(X) + f(c)$$

и сравним коэффициенты при одинаковых степенях X (начиная со старших).

После небольшого преобразования получим

$$\begin{aligned}
&b_0 = a_0,\\
&\cdots\cdots\cdots\\
&b_k = b_{k-1}c + a_k,\\
&\cdots\cdots\cdots\\
&b_{n-1} = b_{n-2}c + a_{n-1},\\
&f(c) = b_{n-1}c + a_n,
\end{aligned}$$

так что заодно вычисляется значение f при $X = c$.

Рекуррентные формулы, в которых и заключается схема Горнера, удобны при счете.

Введем теперь более общее

Определение 2. Элемент $c \in R$ называется k-кратным корней многочлена $f \in R[X]$, если f делится на $(X-c)^k$, но не делится на $(X-c)^{k+1}$.

Корень кратности 1 называют *простым корнем.*

Итак, $c \in R$ — корень кратности k многочлена $f \in R[X]$ тогда и только тогда, когда

$$f(X) = (X-c)^k g(X),$$

где

$$\text{НОД}(X-c, g(X)) = 1.$$

Последнее условие также выражается неравенством $g(c) \neq 0$.

Понятно, что $k \leqslant \deg f$.

Имеет место важная

Теорема 2. *Пусть R — целостное кольцо, $f \neq 0$ — многочлен из $R[X]$, $c_1, \ldots, c_r$ — его корни в R кратностей $k_1, \ldots, k_r$, соответственно.*

Тогда

$$f(X) = (X-c)^{k_1} \ldots (X-c)^{k_r} g(X),$$
$$g(X) \in R[X], \quad g(c_i) \neq 0, \quad i = 1, \ldots, r.$$

В частности, число корней многочлена $f \in R[X]$, рассматриваемых вместе с их кратностями, не превосходит степени многочлена

$$k_1 + k_2 + \cdots + k_r \leqslant \deg f.$$

Доказательство. Достаточно перейти к полю отношений $Q(R)$ (если кольцо R не было полем с самого начала) и воспользоваться однозначностью разложения на простые множители (в данном случае на $X-c_1, \ldots, X-c_r$) в кольце $Q(R)[X]$. Однако в реальности нет необходимости применять такое мощное математическое оружие, будем рассуждать просто и прямо.

Так как

$$\deg f = (k_1 + \cdots + k_r) + \deg g,$$

то искомое неравенство — следствие делимости f на $(X-c_1)^{k_1} \ldots (X-c_r)^{k_r}$, которую мы установим индукцией по r.

При $r = 1$ доказывать нечего.

Пусть мы уже знаем, что

$$f(X) = (X - c_1)^{k_1} \ldots (X - c_{r-1})^{k_{r-1}} h(X).$$

Так как у нас

$$c_r - c_1 \neq 0, \quad \ldots, \quad c_r - c_{r-1} \neq 0$$

и R — целостное кольцо, то элемент c_r не является корнем многочлена

$$(X - c_1)^{k_1} \ldots (X - c_{r-1})^{k_{r-1}}.$$

Но c_r — k_r-кратный корень многочлена f, то есть

$$f(X) = (X - c_r)^{k_r} \cdot u(X).$$

Поэтому $h(c_r) = 0$. Соответственно,

$$h(X) = (X - c_r)^s v(X), \quad s \leqslant k_r.$$

Имеем

$$(X-c_r)^{k_r}u(X) = f(X) = \\ = (X-c_1)^{k_1}\dots(X-c_{r-1})^{k_{r-1}}(X-c_r)^s v(X).$$

Используя закон сокращения в целостном кольце $R[X]$, приходим к заключению, что $s = k_r$. □

Без предположения о целостности кольца R доказанная теорема перестает быть верной, как показывает пример многочлена

$$f(X) = X^3$$

над кольцом $\mathbb{Z}_8$:

$$f(0) = f(2) = f(4) = f(6) = 0.$$

Разложение f на простые множители в $\mathbb{Z}_8$ тоже неоднозначно:

$$f = X^3 = X(X-4)^2 = (X-2)(X^2+2X+4) = (X-6)(X^2-2X+4).$$

Из доказанной нами теоремы вытекает

Следствие 1. *Два многочлена $f, g \in R[X]$ степени $\leqslant n$, принимающие одинаковые значения при подстановке $n+1$ различных элементов из целостного кольца R, равны: $f = g$.*

Доказательство. Положим $h := f - g$, так что $\deg h \leqslant n$. По условию

$$h(c_1) = \dots = h(c_{n+1}) = 0$$

для попарно различных элементов $c_1, \dots, c_{n+1} \in R$, то есть многочлен степени n имеет не менее $n+1$ корней. Противоречие. □

ДИФФЕРЕНЦИРОВАНИЯ КОЛЬЦА МНОГОЧЛЕНОВ

Пусть

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

— многочлен степени n над произвольным полем F. Его *производной* называется многочлен

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}.$$

Если мы имеем дело с полем $\mathbb{R}$, то это определение повторяет определение обычных производной (которую проходят в математическом анализе).

Однако и над произвольным полем имеют место хорошо известные из анализа соотношения

$$(\alpha f + \beta g)' = \alpha f' + \beta g', \quad \alpha, \beta \in F,$$

и

$$(fg)' = f'g + fg'.$$

Первое соотношение проверяется совершенно очевидным образом. Второе благодаря первому можно свести к тому случаю, когда $f = X^k$, $g = X^l$:

$$(X^{k+l})' = (k+l)X^{k+l-1} = (kX^{k-1})X^l + X^k(lX^{l-1}) = \\ = (X^k)'X^l + X^k(X^l)'.$$

Обобщением такой формулы дифференцирования произведения служит легко доказываемая по индукции формула

$$(f_1 f_2 \dots f_k)' = \sum_{i=1}^{k} f_1 \dots f_{i-1} f_i' f_{I+1} \dots f_k.$$

В частности,

$$(f^k)' = k f^{k-1} f'.$$

Будем обозначать отображение дифференцирования через

$$\frac{d}{dX} : f \to f'.$$

Результат m-кратного применения отображения $\frac{d}{dX}$ к $f(X)$ обычно обозначается символом $f^{(m)}(X)$.

Очевидно, что

$$f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n \Longrightarrow f^{(n)}(X) = n! a_0,\ f^{(n+1)}(X) = 0.$$

Если F — поле нулевой характеристики, то

$$\deg f' = \deg f - 1.$$

Однако для полей положительной характеристики p это уже не так, поскольку

$$(X^{kp})' = kpX^{kp-1} = 0.$$

Все же некоторую пользу из рассмотрения производной можно извлечь и в общем случае.

Разделив произвольный многочлен $f \in F[X]$ на $(X-c)^2$, $c \in \widetilde{F}$, $\widetilde{F} \supset F$, а затем записав (линейный) остаток в виде

$$(X-c)s + r, \text{ где } s, r \in \widetilde{F},$$

мы придем к соотношениям

$$f = (X-c)^2 t + (X-c)s + r,$$
$$f' = (X-c)[2t + (X-c)t'] + s.$$

Подставив в них значение $X = c$, получим

$$r = f(c), \quad s = f'(c),$$

то есть

$$f(X) = (X-c)^2 t(X) + (X-c)f'(c) + f(c).$$

Мы пришли к следующему утверждению:

Теорема 3. *Пусть F — произвольное поле, а $\widetilde{F}$ — некоторое его расширение. Многчлен $f \in F[X]$ имеет кратный корень $c \in \widetilde{F}$ тогда и только тогда, когда*

$$f(c) = f'(c) = 0.$$

Предположим, что F — поле нулевой характеристики, и без ограничения общности под F можно понимать одно из полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Нормализованный неприводимый многочлен $p_i(X)$ в разложении

$$f(X) = \lambda p_1(X)^{k_1} \dots p_i(X)^{k_i} \dots p_r(X)^{k_r}, \quad \lambda \in F,$$

многочлена $f(X) \in F[X]$ называется *k_i-кратным множителем* для f.

На практике получить разложение многочлена $f(X)$ в произведение неприводимых довольно сложно. Опишем вкратце метод, основанный на понятии производной и дающий возможность узнать, содержит ли $f(X)$ над данным полем F (или его расширением) кратные множители.

Теорема 4. *Пусть $p(X)$ есть k-кратный неприводимый множитель многочлена $f \in F[X]$ ($k \geqslant 1$, $\deg p(X) \geqslant 1$).*

Тогда $p(X)$ бцдет $(k-1)$-кратным множителем производной $f'(X)$. В частности, при $k = 1$ f' не делится на $p(X)$.

Доказательство. По условию имеем

$$f(X) = p(X)^k g(X),$$

где

$$\text{НОД}(p(X), g(X)) = 1,$$

то есть $g(X)$ не делится на $p(X)$.

Применим правила производной суммы и произведения:

$$f'(X) = p(X)^{k-1}(kp'(X)g(X) + p(X)g'(X)).$$

Достаточно показать, что многочлен в скобках не делится на $p(X)$. Если бы это было не так, то на $p(X)$ делился бы многочлен $kp'(X)g(X)$, что, однако, невозможно, поскольку $g(X)$ не делится на $p(X)$, а

$$\deg kp'(X) < \deg p(X).$$

□

Понятно, что в ходе доказательства существенно были использованы и неприводимость $p(X)$, и условие $\operatorname{char} F = 0$.

Следствие 2. *Для многочлена $f(X)$ коэффициентами в поле F характеристики ноль следующие два условия эквивалентны:*

(1) *f имеет в некотором расщирении $\widetilde{F} \supset F$ поля F корень с кратности k;*

(2) *$f^{(j)}(c) = 0$, $0 \leqslant j \leqslant k-1$, но $f^{(k)}(c) \neq 0$.*

Доказательство. Применим k раз предыдущую теорему, имея в виду линейный множитель $p(X) = X - c$, с самого начала заменяя, в случае необходимости, поле F его расширением $\widetilde{F}$. □

Следствие 3. *Если многочлен $f \in F[X]$ степени $\geqslant 1$ раскладывается в произведение степеней неприводимых:*

$$f(X) = \lambda p_1(X)^{k_1} \dots p_i(X)^{k_i} \dots p_r(X)^{k_r}, \quad \lambda \in F,$$

то разложением для наибольшего общего делителя f и его производной f' будет

$$НОД(f, f') = p_1(X)^{k_1-1} p_2(X)^{k_2-1} \dots p_r(X)^{k_r-1}.$$

Доказательство. Действительно, по доказанной только что теореме каждый из простых делителей $p_i(X)$ многочлена $f(X)$ входит в разложение многочлена $f'(X)$ с показателем $k_i - 1$, то есть

$$f'(X) = p_1(X)^{k_1-1} p_2(X)^{k_2-1} \dots p_r(X)^{k_r-1} \cdot u(X),$$

где

$$\text{НОД}(u, p_i) = 1, \quad 1 \leqslant i \leqslant r.$$

Поэтому получается условие следствия. □

Используя это утверждение про $\text{НОД}(f, f')$, мы получаем средство освободиться от кратных множителей, вхдящих в разложение $f(X)$. Именно, многочлен

$$g(X) = \frac{f(X)}{\text{НОД}(f, f')} = p_1(X) p_2(X) \dots p_r(X)$$

содержит те же простые делители, что и $f(X)$, но с единичной кратностью.

Важно отметить, что многочлен $g(X)$ можно найти, не зная фактически разложений для f и f', а используя лишь алгоритм Евклида.

ФОРМУЛЫ ВИЕТА

Предположим, что нормализованный многочлен $f \in F[X]$ степени n имеет в поле F или в некотором его расширении n корней $c_1, c_2, \ldots, c_n$, среди которых, возможно, есть и одинаковые. Тогда справедливо разложение

$$f(X) = (X - c_1)(X - c_2) \ldots (X - c_n).$$

Запишем, с другой стороны, $f(X)$ в обычном виде по степеням X:

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_k X^{n-k} + \cdots + a_n,$$

а теперь перемножим все члены $X - c_i$ и приведем подобные члены. Тогда для коэффициентов $a_1, \ldots, a_n$ получатся выражения через корни $c_1, \ldots, c_n$:

$$\begin{aligned}
a_1 &= -(c_1 + c_2 + \cdots + c_n), \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
a_k &= (-1)^k \sum_{i_1 < i_2 < \cdots < i_k} c_{i_1} c_{i_2} \ldots c_{i_k}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
a_n &= (-1)^n c_1 c_2 \ldots c_n.
\end{aligned}$$

Эти формулы называются формулами Виета.

Если бы многочлен f не был нормализованным, то есть имел бы старший коффициент $a_0 \neq 1$, то аналогичные формулы давали бы выражение для a_i/a_0.

Формулы Виета, устанавливающие явную связь между корнями и коэффициентами произвольного многочлена, замечательны тем, что их правые части не меняются при любых перестановках корней $c_1, \ldots, c_n$.

Это дает нам повод ввести понятие симметрической функции.

Элемент $\pi \in S_n$ действует на функцию $\widetilde{f}(x_1, \ldots, x_n)$ от n аргументов по правилу

$$\widetilde{(\pi \circ f)}(x_1, \ldots, x_n) = \widetilde{f}(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Функция f называется *симметрической*, если

$$\widetilde{\pi \circ f} = \widetilde{f}$$

для всех $\pi \in S_n$.

Примером симметрических функций служат так называемые *элементарные симметрические многочлены* s_k:

$$s_k(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

Они позволяют переписать формулы Виета в коротком виде

$$a_k = (-1)^k s_k(c_1, \ldots, c_n), \quad k = 1, 2, \ldots, n.$$

Пример 1. Рассмотрим многочлен

$$X^{p-1} - 1$$

над конечным полем $\mathbb{Z}_p$.

Мы знаем, что $x^{p-1} = 1$ для всех $x \in \mathbb{Z}_p^*$, то есть все ненулевые элементы — корни многочлена $X^{p-1} - 1$. Значит, имеет место разложение

$$X^{p-1} - 1 = (X-1)(X-2)\dots(X-(p-1)).$$

Из теоремы Виета получим

$$\begin{aligned} s_k(1,2,\dots,p-1) &\equiv 0 \mod p, \qquad k = 1,2,\dots,p-2, \\ s_{p-1}(1,2,\dots,p-1) &\equiv -1 \mod p. \end{aligned}$$

Последнее соотношение, переписанное в виде

$$(p-1)! + 1 \equiv 0 \mod p$$

и известное под названием *теоремы Вилсона*, выражает фактически необходимый и достаточный признак простоты целого числа p.

Действительно, выполнение того условия для простых p мы только что доказали. С другой стороны,

$$\begin{aligned} p = p_1 p_2 \Longrightarrow (p-1)! = p_1 t \Longrightarrow \\ \Longrightarrow (p-1)! + 1 \not\equiv 0 \mod p_1 \Longrightarrow (p-1)! + 1 \not\equiv 0 \mod p. \end{aligned}$$