§ 19. Многочлены как функции. Корни многочленов

Б.М.Верников

Уральский федеральный университет,
Институт естественных наук и математики,
кафедра алгебры и фундаментальной информатики

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ — многочлен над кольцом R. Многочлен f можно рассматривать как отображение (или, что то же самое, функцию) из кольца R в себя, сопоставляющее каждому элементу $\xi \in R$ элемент $f(\xi) \in R$, определяемый равенством

$$f(\xi) = \alpha_n \xi^n + \alpha_{n-1} \xi^{n-1} + \cdots + \alpha_1 \xi + \alpha_0.$$

Элемент $f(\xi)$ называется *значением многочлена* $f(x)$ в кольце R при $x = \xi$.

В предыдущем параграфе мы, не оговаривая этого в явном виде, имели в виду, что многочлены f и g равны, если у них равны коэффициенты при x^i для всех натуральных i и равны свободные члены. Если вернуться к исходному определению многочлена как бесконечной последовательности неотрицательных целых чисел, это определение можно сформулировать так: многочлены $f = (a_0, a_1, \ldots, a_n, \ldots)$ и $g = (b_0, b_1, \ldots, b_n, \ldots)$ над одним и тем же кольцом R равны, если $a_i = b_i$ для всех $i \geq 0$. В этом случае говорят, что многочлены f и g *равны как последовательности*.

Если же рассматривать многочлены как функции, то можно ввести другое понятие равенства многочленов. Говорят, что многочлены f и g над одним и тем же кольцом R *равны как функции*, если $f(\xi) = g(\xi)$ для любого $\xi \in R$.

Связь между равенством многочленов как последовательностей и их равенством как функций

Возникает естественный вопрос: эквивалентны ли два введенных понятия равенства многочленов? Очевидно, что если многочлены равны как последовательности, то они равны и как функции. В самом деле, в этом случае $f = g = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, и потому $f(\xi) = g(\xi) = a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_0$ для любого $\xi \in R$. Но, как показывает следующий пример, обратная импликация неверна.

Пример многочленов, равных как функции, но не равных как последовательности

Пусть F — конечное поле. В силу леммы о степенях элементов в конечной группе (см. § 4), существует такое натуральное число k, что для любого элемента $\xi \in F \setminus \{0\}$ выполнено равенство $\xi^k = 1$, а значит и равенство $\xi^{k+1} = \xi$. Последнее равенство, очевидно, верно и при $\xi = 0$. Следовательно, оно верно для любого $\xi \in F$. Это означает, что многочлены x^{k+1} и x над полем F равны как функции. В то же время, очевидно, что они различны как последовательности.

В дальнейшем мы увидим, что для многочленов над бесконечным полем примеров такого рода уже не существует, и два введенных выше понятия равенства многочленов эквивалентны (см. следствие о равенстве многочленов ниже в данном параграфе).

Пусть $f(x)$ — многочлен степени $n \geq 1$ над полем F, $\alpha \in F$, а $q(x)$ и $r(x)$ — частное и остаток от деления многочлена $f(x)$ на $x-\alpha$ соответственно. Тогда $\deg r(x) < \deg(x-\alpha) = 1$, т. е. $\deg r(x) \leq 0$. С другой стороны, $\deg\bigl(q(x)(x-\alpha)\bigr) \geq \deg(x-\alpha) = 1$. Учитывая замечание о степени произведения и суммы многочленов, имеем:

$$\begin{aligned}\deg f(x) = \deg\bigl(q(x)(x-\alpha)+r(x)\bigr) = \deg\bigl(q(x)(x-\alpha)\bigr) = \\ = \deg q(x) + \deg(x-\alpha) = \deg q(x)+1,\end{aligned}$$

откуда $\deg q(x) = \deg f(x) - 1 = n-1$.

Теорема Безу

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ — многочлен над полем F и $\alpha \in F$.

(i) *Остаток от деления $f(x)$ на $x-\alpha$ равен $f(\alpha)$.*

(ii) *Обозначим частное от деления $f(x)$ на $x-\alpha$ через $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0$. Тогда*

$$\begin{aligned}&b_{n-1} = a_n,\ b_k = a_{k+1} + \alpha b_{k+1} \text{ при } k = 0, 1, \dots, n-2 \\ &\text{и } f(\alpha) = a_0 + \alpha b_0.\end{aligned} \tag{1}$$

Доказательство. Обозначим частное и остаток от деления $f(x)$ на $x-\alpha$ через $q(x)$ и $r(x)$ соответственно. Тогда $f(x)=q(x)(x-\alpha)+r(x)$, где $\deg r<\deg(x-\alpha)$. Последнее означает, что $\deg r\leqslant 0$, т. е. $r\in F$. Подставив α вместо x в равенство $f(x)=q(x)(x-\alpha)+r(x)$, имеем $f(\alpha)=q(\alpha)\cdot 0+r$, откуда $r=f(\alpha)$. Учитывая, что

$$\begin{aligned}
&a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=\\
&=(b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\cdots+b_1x+b_0)(x-\alpha)+f(\alpha)=\\
&=b_{n-1}x^n+(-\alpha b_{n-1}+b_{n-2})x^{n-1}+\cdots+(-\alpha b_1+b_0)x+\bigl(-\alpha b_0+f(\alpha)\bigr),
\end{aligned}$$

получаем, что $b_{n-1}=a_n$, $-\alpha b_{n-1}+b_{n-2}=a_{n-1}$, ..., $-\alpha b_1+b_0=a_1$, $-\alpha b_0+f(\alpha)=a_0$, откуда вытекают равенства (1). $\square$

На формулах (1) основан упрощенный алгоритм деления многочлена f на двучлен $x-\alpha$ и нахождения значения $f(\alpha)$, известный под названием *схема Горнера*. Для осуществления алгоритма составляется таблица из двух строк. В первой строке записываются коэффициенты многочлена f по убыванию степеней (без пропусков, если некоторая степень отсутствует, то на соответствующем месте записывается нуль). Вторая строка заполняется с учетом формул (1): первое число переносится из первой строки, каждое последующее получается путем умножения предыдущего (только что полученного) числа из второй строки на число α и сложения результата с числом из первой строки, стоящим над заполняемой клеткой второй строки. Последнее число во второй строке (под свободным членом f) и будет значением $f(\alpha)$, а числа с первого по предпоследнее – коэффициентами частного в порядке убывания степеней. Для удобства проведения вычислений число α выписывают слева от первого элемента второй строки.

Определение

Пусть $f(x)$ — многочлен над полем F. Элемент $\alpha \in F$ называется *корнем* многочлена $f(x)$, если $f(\alpha) = 0$ (другими словами, если α — корень уравнения $f(x) = 0$).

Из теоремы Безу вытекает

Следствие из теоремы Безу

Пусть $f(x)$ — многочлен над полем F и $\alpha \in F$. Элемент α является корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = q(x)(x - \alpha)$ для некоторого многочлена $q(x) \in F[x]$.

Доказательство. Необходимость. В силу теоремы Безу,

$$f(x) = q(x)(x - \alpha) + f(\alpha)$$

для некоторого многочлена $q(x)$. Если α — корень многочлена $f(x)$, то $f(\alpha) = 0$, и потому $f(x) = q(x)(x - \alpha)$.

Достаточность. Если $f(x) = q(x)(x - \alpha)$, то

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0.$$

Следствие доказано.

Определение

Натуральное число k называется *кратностью* корня α многочлена $f(x)$, если $f(x) = g(x)(x-\alpha)^k$ для некоторого многочлена $g(x)$ такого, что $g(\alpha) \neq 0$.

Если многочлен $f(x)$ степени > 0 над полем F имеет в этом поле ровно m попарно различных корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ и кратность корня α_i равна k_i, где $i = 1, 2, \ldots, m$, то $f(x)$ делится на $(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m}$. Поэтому $k_1 + k_2 + \cdots + k_m \leqslant \deg f$. Ясно также, что число корней многочлена не превосходит суммы их кратностей. Следовательно, спрведливо следующее утверждение.

Следствие о числе корней и степени многочлена

Как число корней многочлена степени > 0, так и сумма кратностей всех его корней, не могут быть больше степени многочлена. $\square$

Следствие о числе корней и степени многочлена влечет следующее утверждение.

Следствие о равенстве многочленов

Многочлены f и g над бесконечным полем F равны как последовательности тогда и только тогда, когда они равны как функции.

Доказательство. Как уже отмечалось выше в данном параграфе, *необходимость* справедлива для многочленов над произвольным кольцом.

Достаточность. Предположим, что многочлены f и g над бесконечным полем F равны как функции. Пусть $\xi \in F$. Тогда $f(\xi) = g(\xi)$, откуда $(f - g)(\xi) = 0$. Иными словами, любой элемент поля F является корнем многочлена $(f - g)(x)$. Таким образом, этот многочлен имеет бесконечное множество корней. Поскольку, в силу следствия о числе корней и степени многочлена, число корней многочлена степени > 0 не может быть больше степени многочлена, это означает, что $\deg(f - g) \leq 0$. Иными словами, $f - g = \alpha$ для некоторого $\alpha \in F$. При этом $\alpha = 0$, поскольку в противном случае α, вопреки сказанному выше, не является корнем многочлена $f - g$. Иными словами, $f - g = o$, т.е. f и g равны как последовательности. $\square$

Следующее утверждение позволяет отыскивать рациональные корни многочленов с целыми коэффициентами (если они существуют, конечно).

Предложение о рациональных корнях многочленов

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ *— многочлен над* $\mathbb{Q}$ *с целыми коэффициентами, а* $\frac{p}{q}$ *— рациональное число и несократимая дробь. Если* $\frac{p}{q}$ *— корень многочлена* $f(x)$*, то* p *является делителем* a_0*, а* q *— делителем* a_n*. В частности, если* $a_n \in \{1, -1\}$*, то все рациональные корни многочлена* $f(x)$ *являются целыми числами и делят свободный член* a_0*.*

Доказательство. Поскольку $\frac{p}{q}$ — корень многочлена $f(x)$, имеем: $a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \dots + a_1 \cdot \frac{p}{q} + a_0 = 0$. Умножив обе части этого равенства на q^n, получим: $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$. Отсюда получаем: $a_0 q^n = p(-a_n p^{n-1} - a_{n-1} p^{n-2} q - \dots - a_1 q^{n-1})$. Поэтому p делит $a_0 q^n$. Так как числа p и q взаимно просты, p делит a_0. Аналогично, из равенства $a_n p^n = q(-a_{n-1} p^{n-1} - \dots - a_1 p q^{n-2} - a_0 q^{n-1})$ вытекает, что q делит a_n. $\square$

Из предложения, доказанного на предыдущем слайде, непосредственно вытекает

Следствие о целых корнях многочленов

Если $f(x)$ — многочлен над $\mathbb{Q}$ с целыми коэффициентами, старший коэффициент которого равен 1 или -1, то все рациональные корни многочлена $f(x)$ являются целыми числами и делят свободный член этого многочлена. $\square$

Предположим, что мы знаем значения некоторой функции $f(x)$ в $(n+1)$-й точке $x_0, x_1, \ldots, x_n$: $f(x_0) = y_0$, $f(x_1) = y_1$, $\ldots$, $f(x_n) = y_n$, и хотим приблизить эту функцию многочленом. Иными словами, мы хотим найти многочлен $p(x)$ такой, что $p(x_0) = y_0$, $p(x_1) = y_1$, $\ldots$, $p(x_n) = y_n$. Любой многочлен с таким свойством называется *интерполяционным многочленом*, соответствующим набору пар

$$(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n). \tag{2}$$

Многочлен минимальной степени среди интерполяционных многочленов, соответствующих набору пар (2), называется *интерполяционным многочленом Лагранжа*, соответствующим этому набору пар. Оказывается, он всегда существует и определен однозначно.

Теорема об интерполяционном многочлене

Пусть $x_0, x_1, \ldots, x_n$ — попарно различные, а $y_0, y_1, \ldots, y_n$ — произвольные действительные числа. Тогда существует, и притом только один, интерполяционный многочлен Лагранжа $p(x)$, соответствующий набору пар (2), причем $\deg p(x) \leqslant n$.

Доказательство. Для всякого $i = 0, 1, \ldots, n$ положим

$$p_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j} = \frac{x - x_0}{x_i - x_0} \cdots \frac{x - x_{i-1}}{x_i - x_{i-1}} \cdot \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdots \frac{x - x_n}{x_i - x_n}.$$

Очевидно, что $\deg p_i(x) = n$, $p_i(x_i) = 1$ и $p_i(x_j) = 0$ при $j = 0, 1, \ldots, n$, $j \neq i$. Далее, положим $p(x) = y_0 p_0(x) + y_1 p_1(x) + \cdots + y_n p_n(x)$. Очевидно, что $p(x_i) = y_i$ для всякого $i = 0, 1, \ldots, n$. Таким образом, $p(x)$ — интерполяционный многочлен Лагранжа, соответствующий набору пар (2). А из замечания о степени произведения и суммы многочленов (см. § 18) вытекает, что $\deg p(x) \leqslant n$.

Предположим, что $q(x)$ — отличный от $p(x)$ интерполяционный многочлен, соответствующий набору пар (2). Положим $r(x) = p(x) - q(x)$. Тогда $r(x) \neq o$ и $r(x_i) = p(x_i) - q(x_i) = y_i - y_i = 0$ для всех $i = 0, 1, \ldots, n$. Иными словами, $x_0, x_1, \ldots, x_n$ — попарно различные корни многочлена $r(x)$. В силу следствия о числе корней и степени многочлена, $\deg r(x) \geqslant n + 1 > \deg p(x)$. Таким образом, степень многочлена $p(x)$ меньше степени любого другого интерполяционного многочлена, соответствующего набору пар (2). Следовательно, $p(x)$ — единственный интерполяционный многочлен Лагранжа, соответствующий этому набору пар. ☐