§ 18. Многочлены как функции. Корни многочленов

Б.М.Верников

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

18.1. Аппроксимация функций многочленами

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ — многочлен над кольцом R. Его можно рассматривать как отображение 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 $f(\xi)$ кольца R называется *значением многочлена* $f(x)$ в кольце R при $x = \xi$ (или в точке x).

В различных приложениях математики часто возникает следующая задача. Исследуется некоторая функция (отображение) $f(x)$ из поля F в себя. Известны значения функции $f(x)$ в точках x_0, x_1, …, x_n: $f(x_0) = y_0$, $f(x_1) = y_1$, …, $f(x_n) = y_n$. Требуется аппроксимировать (приблизить) эту функцию многочленом, т. е. найти многочлен $p(x)$ наименьшей возможной степени над полем F такой, что $p(x_0) = y_0$, $p(x_1) = y_1$, …, $p(x_n) = y_n$. Любой многочлен с таким свойством называется *интерполяционным многочленом Лагранжа*, соответствующим набору пар

$$(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n). \tag{1}$$

Интерполяционный многочлен Лагранжа (2)

Следующая теорема показывает, что интерполяционный многочлен Лагранжа, соответствующий любому набору пар (1), существует и определен однозначно. Кроме того, она показывает, что всякий многочлен степени $\leqslant n$ над данным полем однозначно определяется своими значениями в $(n+1)$-й точке.

Теорема 18.1

Пусть F — поле, содержащее $> n$ элементов, $\xi_0, \xi_1, \ldots, \xi_n$ — попарно различные элементы поля F, а $\alpha_0, \alpha_1, \ldots, \alpha_n$ — его произвольные элементы. Тогда существует, и притом только один, многочлен $p(x)$ степени $\leqslant n$ над полем F такой, что $p(\xi_i) = \alpha_i$ для всех $i = 0, 1, \ldots, n$.

Доказательство. Пусть $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ — произвольный многочлен над полем F. Если $p(\xi_i) = \alpha_i$ для всех $i = 0, 1, \ldots, n$, то выполнены равенства

$$\begin{cases} a_n \xi_0^n + a_{n-1} \xi_0^{n-1} + \cdots + a_0 = \alpha_0, \\ a_n \xi_1^n + a_{n-1} \xi_1^{n-1} + \cdots + a_0 = \alpha_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_n \xi_n^n + a_{n-1} \xi_n^{n-1} + \cdots + a_0 = \alpha_n. \end{cases}$$

Интерполяционный многочлен Лагранжа (3)

Это означает, что набор скаляров $(a_0, a_1, \ldots, a_n)$ является решением системы линейных уравнений

$$\begin{cases} x_0 + \xi_0 x_1 + \xi_0^2 x_2 + \cdots + \xi_0^n x_n = \alpha_0, \\ x_0 + \xi_1 x_1 + \xi_1^2 x_2 + \cdots + \xi_1^n x_n = \alpha_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_0 + \xi_n x_1 + \xi_n^2 x_2 + \cdots + \xi_n^n x_n = \alpha_n. \end{cases} \tag{2}$$

Таким образом, доказываемое утверждение равносильно тому, что система (2) имеет решение, и притом только одно.

Докажем, что это так. Система (2) является крамеровской, а ее определителем является определитель Вандермонда

$$V(\xi_0, \xi_1, \ldots, \xi_n) = \begin{vmatrix} 1 & \xi_0 & \xi_0^2 & \ldots & \xi_0^n \\ 1 & \xi_1 & \xi_1^2 & \ldots & \xi_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \xi_n & \xi_n^2 & \ldots & \xi_n^n \end{vmatrix}.$$

Поскольку по условию скаляры $\xi_0, \xi_1, \ldots, \xi_n$ попарно различны, $V(\xi_0, \xi_1, \ldots, \xi_n) \neq 0$ в силу следствия 7.5. Из теоремы Крамера теперь вытекает, что система (2) имеет решение, причем ровно одно. □

Интерполяционный многочлен Лагранжа (4)

Доказательство теоремы 18.1 указывает способ построения интерполяционного многочлена Лагранжа, соответствующего набору пар (1): чтобы найти его коэффициенты, надо решить систему (2). Укажем еще один способ построения этого многочлена. Для всякого $i = 0, 1, \ldots, n$ положим

$$p_i(x) = \frac{x - x_0}{x_i - x_0} \cdot \frac{x - x_1}{x_i - x_1} \cdot \ldots \cdot \frac{x - x_{i-1}}{x_i - x_{i-1}} \cdot \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdot \ldots \cdot \frac{x - x_n}{x_i - x_n}. \qquad (3)$$

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

$$p(x) = y_0 p_0(x) + y_1 p_1(x) + \cdots + y_n p_n(x). \qquad (4)$$

Тогда для всякого $i = 0, 1, \ldots, n$ выполнены равенства

$$\begin{aligned} p(x_i) &= y_0 p_0(x_i) + y_1 p_1(x_i) + \cdots + y_{i-1} p_{i-1}(x_i) + \\ &+ y_i p_i(x_i) + y_{i+1} p_{i+1}(x_i) + \cdots + y_n p_n(x_i) = \\ &= y_0 \cdot 0 + y_1 \cdot 0 + \cdots + y_{i-1} \cdot 0 + y_i \cdot 1 + \\ &+ y_{i+1} \cdot 0 + \cdots + y_n \cdot 0 = y_i. \end{aligned}$$

При этом ясно, что $\deg p(x) \leqslant n$.

Интерполяционный многочлен Лагранжа (5)

Из теоремы 18.1 вытекает, что других многочленов степени $\leqslant \deg p(x)$, которые в точках $x_0, x_1, \ldots, x_n$ принимали бы значения $y_0, y_1, \ldots, y_n$ соответственно, не существует. Следовательно, $p(x)$ — интерполяционный многочлен, соответствующий набору пар (1).

Интерполяционные многочлены Лагранжа будут использоваться в § 19 при изучении многочленов над полем $\mathbb{Q}$, разложимых в произведение многочленов меньших степеней.

18.2. Два понятия равенства многочленов

Всюду ранее мы, не оговаривая этого в явном виде, имели в виду, что многочлены f и g равны, если у них равны коэффициенты при x^k для всех натуральных k и равны свободные члены. Если вернуться к исходному определению многочлена как бесконечной последовательности элементов некоторого кольца, то это определение равенства многочленов можно сформулировать так: многочлены $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ и $g = (\beta_0, \beta_1, \ldots, \beta_n, \ldots)$ над одним и тем же кольцом R равны, если $\alpha_i = \beta_i$ для всех $i \geqslant 0$. В этом случае говорят, что многочлены f и g *равны как последовательности*.

- *Запись $f = g$ всюду в дальнейшем будет означать (как и всюду ранее означала), 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 $\xi \in R$. Возникает естественный вопрос: эквивалентны ли два введенных понятия равенства многочленов?

Два понятия равенства многочленов (2)

Замечание 18.1

Если многочлены f и g над одним и тем же ассоциативно-коммутативным кольцом R с 1 равны как последовательности, то они равны и как функции.

Доказательство. По условию $f = g = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ для некоторых $\alpha_0, \alpha_1, \ldots, \alpha_n \in R$, и потому $f(\xi) = g(\xi) = \alpha_n \xi^n + \alpha_{n-1} \xi^{n-1} + \cdots + \alpha_0$ для любого $\xi \in R$. □

Но, как показывает следующий пример, обратная импликация в общем случае неверна.

Пример 18.1

Очевидно, что если x — произвольный элемент поля $\mathbb{Z}_2 = \{0, 1\}$, то выполнено равенство $x^2 = x$. Следовательно, многочлены x^2 и x над полем $\mathbb{Z}_2$ равны как функции. В то же время, очевидно, что они не равны как последовательности.

Аналогичный пример можно построить для многочленов над произвольным конечным полем.

Два понятия равенства многочленов (3)

Но, как показывает следующее утверждение, для многочленов над бесконечным полем примеров такого рода не существует.

Предложение 18.1

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

Доказательство. *Необходимость* вытекает из замечания 18.1.

Достаточность. Положим $n = \max\{\deg f, \deg g\}$. Поскольку поле F бесконечно, существуют попарно различные скаляры $\xi_0, \xi_1, \ldots, \xi_n \in F$. При этом $f(\xi_i) = g(\xi_i)$ для всех $i = 0, 1, \ldots, n$, поскольку многочлены f и g равны как функции. Для всякого $i = 0, 1, \ldots, n$ положим $f(\xi_i) = g(\xi_i) = \alpha_i$. Тогда f и g — интерполяционные многочлены, соответствующие набору пар (ξ_0, α_0), (ξ_1, α_1), $\ldots$, (ξ_n, α_n) и $\deg f, \deg g \leqslant n$. Но по теореме 18.1 существует только один многочлен с такими свойствами. Следовательно, $f = g$. □

18.3. Корни многочленов над произвольным полем

Следующее утверждение будет часто использоваться в дальнейшем.

Теорема 18.2 (теорема Безу)

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *— многочлен степени* > 0 *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:*

(i) $r(x) = f(\alpha)$;

(ii) $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$, *где* $b_{n-1} = a_n$ *и* $b_k = a_{k+1} + \alpha b_{k+1}$ *для всех* $k = 0, 1, \ldots, n-2$.

Доказательство. (i) По условию, $f(x) = q(x)(x - \alpha) + r(x)$, где $\deg r < \deg(x - \alpha)$. Поскольку $\deg(x - \alpha) = 1$, получаем, что $\deg r(x) \leqslant 0$, т. е. $r(x) \in F$. Таким образом, $r(x)$ — скаляр, не зависящий от x. Поэтому далее вместо $r(x)$ будем писать r. Подставив α вместо x в равенство $f(x) = q(x)(x - \alpha) + r$, имеем $f(\alpha) = q(\alpha) \cdot 0 + r$, откуда $r = f(\alpha)$.

Теорема Безу (2)

(ii) Ясно, что $\deg\big(q(x)(x-\alpha)\big) \geqslant \deg(x-\alpha) = 1 > \deg r$. Учитывая замечание 17.2, имеем:

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

откуда $\deg q(x) = \deg f(x) - 1 = n-1$. Следовательно, $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$ для некоторых $b_0, b_1, \ldots, b_{n-1} \in F$. Учитывая, что $r = f(\alpha)$ в силу п. (i), имеем:

$$\begin{aligned}a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \\ = (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0)(x-\alpha) + f(\alpha) = \\ = b_{n-1}x^n + (-\alpha b_{n-1} + b_{n-2})x^{n-1} + \cdots + (-\alpha b_1 + b_0)x + \\ + \big(-\alpha b_0 + f(\alpha)\big).\end{aligned}$$

Следовательно, $b_{n-1} = a_n$, $-\alpha b_{n-1} + b_{n-2} = a_{n-1}$, $\ldots$, $-\alpha b_1 + b_0 = a_1$, $-\alpha b_0 + f(\alpha) = a_0$, откуда вытекают все требуемые равенства. □

Схема Горнера

Понятно, что многочлен $f(x)$ можно разделить на двучлен $x - \alpha$ «напрямую», т. е. столбиком. Но теорема Безу позволяет указать более компактный и удобный способ решения этой задачи. Этот способ известен как *схема Горнера*. Он состоит в следующем. Требуется найти частное $q(x)$ и остаток $r(x)$ от деления многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ на двучлен $x - \alpha$. Составим таблицу из двух строк. В первой строке запишем коэффициенты многочлена $f(x)$ в порядке убывания их индексов: a_n, a_{n-1}, ..., a_1, a_0. В первую клетку второй строки перенесем число из первой клетки первой строки. Каждое последующее число второй строки будем вычислять путем умножения предыдущего (только что найденного) числа из второй строки на α и сложения результата с числом из первой строки, стоящим над заполняемой клеткой второй строки. Согласно теореме Безу, в результате указанных действий во всех клетках второй строки, кроме последней, слева направо будут выписаны коэффициенты многочлена $q(x)$ в порядке убывания индексов, а в ее последней клетке будет стоять скаляр, равный $r(x)$. Обычно, для удобства проведения вычислений, скаляр α записывают во второй строке слева от ее первого элемента.

Корень многочлена. Следствие из теоремы Безу

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 18.1 (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 $f(x) = q(x)(x - \alpha)$. Из п. (ii) теоремы Безу вытекает, что $q(x) \in F[x]$.

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

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

□

Кратность корня многочлена

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 $g(\alpha) \neq 0$. Корень многочлена называется *кратным*, если его кратность > 1, и *простым*, если она равна 1. Чтобы упростить рассуждения, нам будет иногда удобно рассматривать скаляр, не являющийся корнем многочлена f, как корень f *кратности* 0.

Пусть $f(x)$ — многочлен степени > 0 над полем F, а $\alpha_1, \alpha_2, \ldots, \alpha_m$ — его попарно различные корни в этом поле. Для всякого $i = 1, 2, \ldots, m$ обозначим через k_i кратность корня α_i. Тогда $f(x)$ делится на $(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m}$, и потому $k_1 + k_2 + \cdots + k_m \leqslant \deg f$. Учитывая еще, что число корней многочлена не превосходит суммы их кратностей, получаем, что справедливо следующее утверждение.

Следствие 18.2

Пусть f — многочлен степени $n > 0$ над полем F. Сумма кратностей всех корней многочлена f, а значит, и число его корней не превосходит n. В частности, число корней многочлена f конечно. □

18.4. Корни многочленов над полем $\mathbb{C}$

Оставшаяся часть параграфа посвящена изучению корней многочленов над тремя основными числовыми полями: $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$. Начнем с самого большого из них — поля комплексных чисел. Здесь ключевую роль играет следующий фундаментальный факт.

Теорема 18.3 (основная теорема алгебры)

Любой многочлен степени > 0 над полем $\mathbb{C}$ имеет по крайней мере один комплексный корень. □

Доказательство этой теоремы выходит за рамки нашего курса, и потому мы не будем его приводить.

Основная теорема алгебры (комментарии)

- Основная теорема алгебры — пример «чистой теоремы существования»: ни сама эта теорема, ни ее доказательство не дают никакой информации о том, как искать комплексные корни многочленов над полем $\mathbb{C}$.
- Свой громкий титул («основная теорема алгебры») эта теорема получила в конце XVIII века, когда она была доказана Гауссом. В то время он соответствовал действительности, поскольку решение алгебраических уравнений, т. е. поиск корней многочленов, рассматривалось тогда как основная задача алгебры. Сейчас это название следует воспринимать только как традиционное и историческое.

Разложимость многочленов над $\mathbb{C}$ на линейные множители

Пусть f — многочлен над $\mathbb{C}$ и $\deg f = n > 0$. По основной теореме алгебры многочлен f имеет некоторый корень α_1. Но тогда, по следствию из теоремы Безу, $f(x) = (x - \alpha_1)g(x)$ для некоторого многочлена g. Ясно, что $\deg g = n - 1$. Если $n - 1 > 0$, то по основной теореме алгебры многочлен g имеет некоторый корень α_2, и потому

$$f(x) = (x - \alpha_1)g(x) = (x - \alpha_1)(x - \alpha_2)h(x)$$

для некоторого многочлена h степени $n - 2$. Продолжая этот процесс, мы через n шагов представим f в виде произведения n линейных множителей и многочлена нулевой степени (т. е. элемента поля $\mathbb{C}$). Иными словами,

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = (ax - a\alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

где $a, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Таким образом, справедливо

Следствие 18.3

Любой многочлен степени $n > 0$ над полем $\mathbb{C}$ разложим в произведение n линейных множителей. □

Число комплексных корней многочлена над полем $\mathbb{C}$

Из следствия 18.3 вытекает

Следствие 18.4

Любой многочлен степени $n > 0$ над полем $\mathbb{C}$ имеет ровно n комплексных корней, если каждый корень считать столько раз, какова его кратность. □

То же самое утверждение можно переформулировать следующим образом:

!! *сумма кратностей всех корней многочлена степени > 0 над полем $\mathbb{C}$ равна степени этого многочлена.* □

Лемма о модуле старшего члена (1)

Для дальнейшего нам понадобится следующее несложное наблюдение.

Лемма 18.1 (лемма о модуле старшего члена)

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен степени* > 0 *над полем* $\mathbb{C}$, *а* k *— произвольное положительное действительное число. Положим* $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. *Если* $\xi \in \mathbb{C}$ *и* $|\xi| \geqslant \frac{kA}{|a_n|} + 1$, *то*

$$|a_n \xi^n| > k \cdot |a_{n-1}\xi^{n-1} + \cdots + a_1 \xi + a_0|. \tag{5}$$

- Поскольку в формулировке леммы речь идет о многочлене над полем $\mathbb{C}$, под модулем здесь понимается модуль комплексного числа.
- Лемма о модуле старшего члена говорит о том, что при достаточно больших по модулю значениях x модуль старшего члена многочлена становится в любое наперед заданное число раз больше модуля суммы всех остальных его членов.

Лемма о модуле старшего члена (2)

Доказательство. В самом деле:

$$
\begin{aligned}
&|a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0| \\
&\leqslant |a_{n-1}\xi^{n-1}| + \cdots + |a_1\xi| + |a_0| && \text{поскольку } |x+y| \leqslant |x| + |y| \\
&= |a_{n-1}| \cdot |\xi|^{n-1} + \cdots + |a_1| \cdot |\xi| + |a_0| && \text{поскольку } |xy| = |x| \cdot |y| \\
&\leqslant A\big(|\xi|^{n-1} + \cdots + |\xi| + 1\big) && \text{по определению числа } A \\
&= A \cdot \frac{|\xi|^n - 1}{|\xi| - 1} && \text{по формуле суммы первых } n \text{ членов} \\
& && \text{геометрической прогрессии} \\
&\leqslant A \cdot \frac{\big(|\xi|^n - 1\big) \cdot |a_n|}{kA} && \text{поскольку } |\xi| - 1 \geqslant \frac{kA}{|a_n|} \\
&= \frac{|a_n| \cdot \big(|\xi|^n - 1\big)}{k} \\
&< \frac{|a_n| \cdot |\xi|^n}{k} \\
&= \frac{|a_n\xi^n|}{k} && \text{поскольку } |xy| = |x| \cdot |y|.
\end{aligned}
$$

Итак, $|a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0| < \frac{|a_n\xi^n|}{k}$. Поскольку $k > 0$, это эквивалентно неравенству (5).

Предложение о модуле корня многочлена

Для произвольного многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ степени > 0 над полем $\mathbb{C}$ положим

$$R_f = \frac{\max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}}{|a_n|} + 1.$$

Предложение 18.2

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ — многочлен степени > 0 над полем $\mathbb{C}$. Если ξ — корень многочлена $f(x)$, то $|\xi| < R_f$.

Доказательство. Если $\xi \in \mathbb{C}$ и $|\xi| \geqslant R_f$, то, применяя неравенство (5) при $k = 1$, получаем, что

$$|a_n \xi^n| > |a_{n-1} \xi^{n-1} + \cdots + a_1 \xi + a_0|,$$

и потому $f(\xi) = a_n \xi^n + a_{n-1} \xi^{n-1} + \cdots + a_1 \xi + a_0 \neq 0$. Следовательно, если ξ — корень многочлена $f(x)$, то $|\xi| < R_f$. □

Корень многочлена на комплексной плоскости

В терминах упоминавшейся в § 4 геометрической интерпретации комплексных чисел предложение 18.2 можно переформулировать следующим образом: корень ξ многочлена f над полем $\mathbb{C}$ располагается на комплексной плоскости внутри круга радиуса R_f с центром в начале координат. Этот факт проиллюстрирован на рис. 1. Окружность, ограничивающая упомянутый круг, изображена пунктирной линией, поскольку ξ не может лежать на ней.

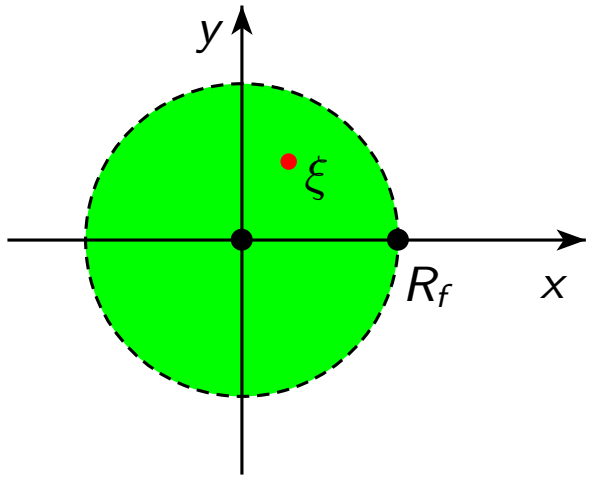

Рис. 1. Корень ξ многочлена f на комплексной плоскости

Лемма о корнях и комплексной сопряженности (1)

Завершая изучение корней многочленов над полем $\mathbb{C}$, докажем следующую лемму, которая будет использоваться в дальнейшем.

Лемма 18.2

Пусть $f(x)$ — многочлен над полем $\mathbb{C}$, все коэффициенты которого являются действительными числами, а γ — корень этого многочлена. Тогда число $\overline{\gamma}$ является корнем многочлена $f(x)$ той же кратности, что и γ.

Доказательство. Пусть $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$. Тогда $\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0 = 0$. Используя свойства операции сопряжения комплексных чисел и тот факт, что $\overline{\alpha} = \alpha$ для всякого $\alpha \in \mathbb{R}$, имеем:

$$
\begin{aligned}
f(\overline{\gamma}) &= \alpha_n \overline{\gamma}^{\,n} + \alpha_{n-1} \overline{\gamma}^{\,n-1} + \cdots + \alpha_1 \overline{\gamma} + \alpha_0 = \\
&= \overline{\alpha_n} \cdot \overline{\gamma}^{\,n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma}^{\,n-1} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} = \\
&= \overline{\alpha_n} \cdot \overline{\gamma^n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma^{n-1}} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} = \\
&= \overline{\alpha_n \gamma^n} + \overline{\alpha_{n-1} \gamma^{n-1}} + \cdots + \overline{\alpha_1 \gamma} + \overline{\alpha_0} = \\
&= \overline{\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0} = \overline{0} = 0.
\end{aligned}
$$

Мы доказали, что $\overline{\gamma}$ — корень многочлена $f(x)$.

Лемма о корнях и комплексной сопряженности (2)

Осталось проверить, что γ и $\overline{\gamma}$ — корни многочлена $f(x)$ одной и той же кратности. В самом деле, предположим, что γ — корень $f(x)$ кратности k, $\overline{\gamma}$ — корень $f(x)$ кратности m и $k \neq m$. Для определенности будем считать, что $k > m$. Положим $g(x) = (x-\gamma)(x-\overline{\gamma}) = x^2 - (\gamma+\overline{\gamma})x + \gamma\overline{\gamma}$. Поскольку $\gamma+\overline{\gamma}, \gamma\overline{\gamma} \in \mathbb{R}$ для любого $\gamma \in \mathbb{C}$, получаем, что $g(x)$ — многочлен с действительными коэффициентами. Ясно, что $g^m \mid f$. Иными словами, $f = g^m h$ для некоторого многочлена h. Как частное многочленов с действительными коэффициентами, многочлен h также имеет действительные коэффициенты. При этом ясно, что h делится на $(x-\gamma)^{k-m}$, поскольку f делится на $(x-\gamma)^k$. Следовательно, γ — корень многочлена h. В силу сказанного выше число $\overline{\gamma}$ также является корнем h. Но тогда $\overline{\gamma}$ — корень многочлена f кратности $> m$. Полученное противоречие завершает доказательство. $\square$

18.5. Действительные корни многочленов над полем $\mathbb{R}$

Перейдем к рассмотрению действительных корней многочленов над полем $\mathbb{R}$. Прежде всего, отметим, что аналог основной теоремы алгебры в данном случае места не имеет: действительные корни есть не у всех многочленов из $\mathbb{R}[x]$. Очевидным примером, подтверждающим это, является многочлен x^2+1. Заметим, что он имеет четную степень. Это не случайно, поскольку справедливо следующее утверждение.

Предложение 18.3

Любой многочлен нечетной степени над полем $\mathbb{R}$ имеет по крайней мере один действительный корень.

Доказательство. Мы приведем два принципиально различных доказательства этого утверждения. Первое из них опирается на факты из математического анализа, второе является чисто алгебраическим.

Аналитическое доказательство предложения 18.3 (1)

Аналитическое доказательство. Как известно из математического анализа, многочлены над $\mathbb{R}$ являются непрерывными функциями из $\mathbb{R}$ в $\mathbb{R}$. Это позволяет нам в дальнейшем использовать следующую теорему Больцано–Коши: если функция g из $\mathbb{R}$ в $\mathbb{R}$ непрерывна на отрезке $[c, d]$ и числа $g(c)$ и $g(d)$ имеют разные знаки, то $g(\xi) = 0$ для некоторого $\xi \in (c, d)$ (см. рис. 2).

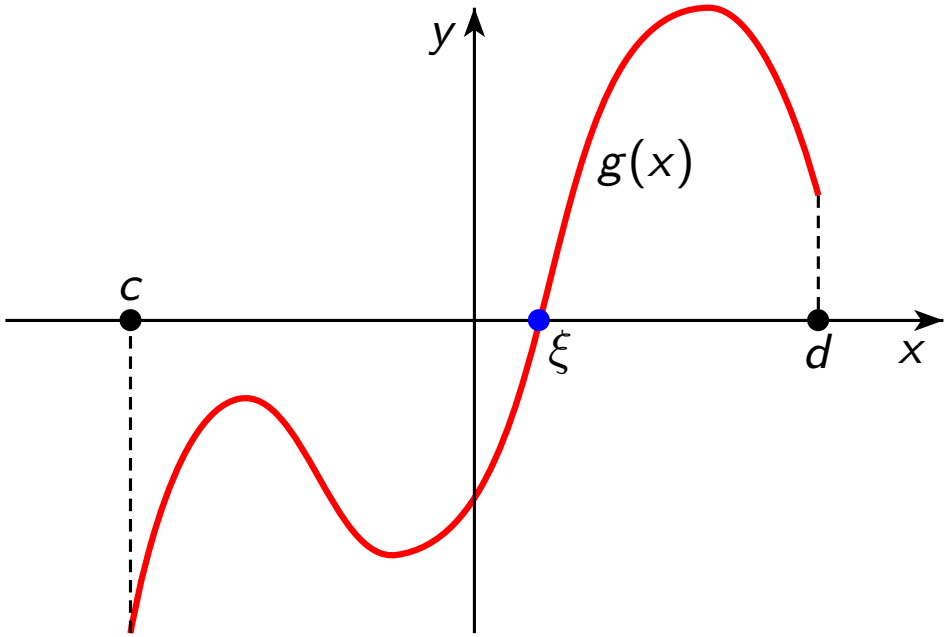

Рис. 2. Корень ξ на отрезке $[c, d]$

Аналитическое доказательство предложения 18.3 (2)

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ — многочлен нечетной степени над полем $\mathbb{R}$. Можно считать, что $a_n > 0$, так как в противном случае можно умножить $f(x)$ на -1 (понятно, что при этом корни многочлена не изменятся). Пусть c и d — действительные числа такие, что $c < -R_f$ и $d > R_f$. Применяя неравенство (5) при $k = 1$, получаем, что $f(c) \neq 0$ и знак числа $f(c)$ совпадает со знаком числа $a_n c^n$. Учитывая, что $a_n > 0$, $c < 0$, а число n нечетно, получаем, что $f(c) < 0$. Аналогично проверяется, что $f(d) > 0$. Из упомянутой на предыдущем слайде теоремы Больцано–Коши вытекает, что $f(\xi) = 0$ для некоторого $\xi \in (c, d)$. □

Алгебраическое доказательство предложения 18.3

Алгебраическое доказательство. Пусть f — многочлен над полем $\mathbb{R}$. В силу следствия 18.4 степень многочлена f равна числу его корней, подсчитываемых с учетом их кратностей. А из леммы 18.2 вытекает, что корни, не являющиеся действительными числами, можно разбить на пары комплексно сопряженных друг к другу чисел, и потому число таких корней четно. Следовательно, если степень многочлена f нечетна, то среди его корней должны быть действительные числа. $\square$

Возникает естественный вопрос о том, как искать действительные корни уравнений вида $f(x) = 0$, где $f(x) \in \mathbb{R}[x]$. Если $\deg f = 1$, то ответ на него очевиден: уравнение $ax + b = 0$, где $a \neq 0$, решается по формуле $x = -\frac{b}{a}$. Из школьного курса математики хорошо известна формула для вычисления корней квадратного уравнения, которая дает ответ на поставленный вопрос в случае, когда $\deg f = 2$. В XVI в. были найдены формулы для вычисления корней уравнений степени 3 и 4. Однако в начале XIX в. было показано, что аналогичных формул для уравнений степени $\geqslant 5$ не существует.

Таким образом, не существует способа найти все действительные корни произвольного многочлена над полем $\mathbb{R}$. Оказывается, однако, что можно получить существенную информацию о корнях многочлена $f(x) \in \mathbb{R}[x]$, не находя их. В частности, из предложения 18.2 немедленно вытекает

Следствие 18.5

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен степени* > 0 *над полем* $\mathbb{R}$. *Если* ξ *— корень многочлена* $f(x)$, *то* $-R_f < \xi < R_f$. □

Кратность корня многочлена и его производной (1)

Кроме того, для произвольного многочлена над полем $\mathbb{R}$ можно найти число всех действительных корней этого многочлена и число его корней, принадлежащих произвольному наперед заданному отрезку числовой прямой. Как мы увидим ниже, это открывает путь к приближенному вычислению корней многочленов над $\mathbb{R}$ с любой наперед заданной степенью точности. Чтобы доказать соответствующие результаты, нам понадобятся некоторые новые понятия и вспомогательные утверждения.

Как обычно, через f' обозначается производная многочлена f над полем $\mathbb{R}$.

Лемма 18.3

Пусть f — многочлен над полем $\mathbb{R}$, а ξ — действительный корень многочлена f кратности k. Если $k = 1$, то ξ не является корнем многочлена f'. Если $k > 1$, то ξ является корнем многочлена f' кратности $k - 1$.

Доказательство. По условию f делится на $(x - \xi)^k$, т. е. $f(x) = (x - \xi)^k g(x)$ для некоторого многочлена $g(x)$, но f не делится на $(x - \xi)^{k+1}$. Если $k = 1$, то $f(x) = (x - \xi)g(x)$ и g не делится на $x - \xi$ (в противном случае f делился бы на $(x - \xi)^2$). Тогда $f' = g + (x - \xi)g'$.

Кратность корня многочлена и его производной (2)

Если ξ — корень многочлена f', то в силу следствия из теоремы Безу f' делится на $x-\xi$. Тогда из равенства $f' = g + (x-\xi)g'$ вытекает, что g делится на $x-\xi$. Но, как отмечалось выше, это не так. Итак, если $k=1$, то ξ не является корнем многочлена f'.

Пусть теперь $k > 1$. Тогда

$$f' = k(x-\xi)^{k-1}g + (x-\xi)^k g' = (x-\xi)^{k-1}(kg + (x-\xi)g').$$

Чтобы завершить доказательство, осталось проверить, что многочлен $kg + (x-\xi)g'$ не делится на $x-\xi$. В самом деле, если $kg + (x-\xi)g'$ делится на $x-\xi$, то $(x-\xi) \mid (kg)$, т. е. $kg = (x-\xi)h$ для некоторого многочлена h. Но тогда $g = \frac{h}{k}(x-\xi)$, т. е. $(x-\xi) \mid g$. Это означает, что f делится на $(x-\xi)^{k+1}$ вопреки условию. □

Переход к многочлену без кратных корней

Из леммы 18.3 вытекает следующее утверждение.

Следствие 18.6

Пусть f — произвольный многочлен степени > 0 над полем $\mathbb{R}$. Положим $g = \frac{f}{d}$, где d — наибольший общий делитель многочленов f и f'. Многочлены f и g имеют одни и те же корни, причем второй из них не имеет кратных корней.

Доказательство. Очевидно, что все корни многочлена g являются корнями многочлена f. А в силу леммы 18.3 все корни многочлена f являются простыми корнями многочлена g. □

Лемма 18.3 и следствие 18.6 будут обобщены в § 19 (см. предложение 19.3 и следствие 19.1 соответственно).

Корень многочлена и производные высших степеней

Следуя обозначениям, принятым в математическом анализе, для всякого натурального $k \geqslant 4$ будем обозначать k-ю производную многочлена f через $f^{(k)}$. Отметим еще одно полезное следствие леммы 18.3.

Следствие 18.7

Действительное число ξ является корнем кратности k многочлена f над полем $\mathbb{R}$ тогда и только тогда, когда оно является корнем многочленов f, f', f'', $\ldots$, $f^{(k-1)}$, но не является корнем многочлена $f^{(k)}$. □

Система многочленов Штурма (1)

Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$. Положим $f_0 = f$ и $f_1 = f'$. Разделим f_0 на f_1 с остатком и обозначим через f_2 остаток от деления, умноженный на -1. Таким образом, $f_0 = q_1 f_1 - f_2$ для некоторого многочлена q_1 и $\deg f_2 < \deg f_1$. Если $f_2 \neq o$, разделим f_1 на f_2 с остатком и обозначим через f_3 остаток от деления, умноженный на -1. Таким образом, $f_1 = q_2 f_2 - f_3$ для некоторого многочлена q_2 и $\deg f_3 < \deg f_2$. Если $f_3 \neq o$, продолжим этот процесс. Поскольку $\deg f_1 > \deg f_2 > \deg f_3 > \cdots$, через конечное число шагов степень очередного остатка окажется $\leqslant 0$. Если сам остаток при этом будет отличен от o, то он станет равным o на следующем шаге. Мы получим следующую систему равенств:

$$\begin{cases} f_0 = q_1 f_1 - f_2, \ f_2 \neq o, \ \deg f_2 < \deg f_1; \\ f_1 = q_2 f_2 - f_3, \ f_3 \neq o, \ \deg f_3 < \deg f_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_{m-2} = q_{m-1} f_{m-1} - f_m, \ f_m \neq o, \ \deg f_m < \deg f_{m-1}; \\ f_{m-1} = q_m f_m. \end{cases}$$

Определение

Упорядоченная последовательность многочленов $f_0, f_1, \ldots, f_m$ называется *системой многочленов Штурма* для многочлена f.

Система многочленов Штурма (2)

Лемма 18.4

Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$, а $f_0, f_1, \ldots, f_m$ — система многочленов Штурма для многочлена f. Тогда:

а) *f_m — наибольший общий делитель многочленов f и f';*

б) *многочлен f не имеет кратных корней тогда и только тогда, когда f_m не имеет действительных корней.*

Если f не имеет кратных корней, то, кроме того:

в) *для всякого $i = 0, 1, \ldots, m-1$ многочлены f_i и f_{i+1} не имеют общих действительных корней;*

г) *если $f_k(\xi) = 0$ для некоторого $\xi \in \mathbb{R}$ и некоторого $0 < k < m$, то числа $f_{k-1}(\xi)$ и $f_{k+1}(\xi)$ имеют разные знаки.*

Система многочленов Штурма (3)

Доказательство. а) Процесс построения системы многочленов Штурма очень близок к процессу нахождения наибольшего общего делителя двух многочленов по алгоритму Евклида (см. доказательство теоремы 17.2). Отличие состоит лишь в том, что при построении системы многочленов Штурма мы на каждом шаге умножаем остаток от деления на -1. Но умножение на ненулевую константу никак не влияет на делимость многочленов. Следовательно, f_m — наибольший общий делитель многочленов f и f'. Отметим, что этот факт можно доказать и непосредственно, дословно повторив доказательство теоремы 17.2.

б) *Необходимость.* Если многочлен f_m имеет действительный корень ξ, то в силу следствия из теоремы Безу $(x - \xi) \mid f_m$. Поскольку, в силу п. а), f_m — наибольший общий делитель многочленов f и f', мы получаем, что $x - \xi$ делит и f, и f', и потому ξ является корнем обоих этих многочленов. Но тогда, в силу леммы 18.3, ξ является кратным корнем многочлена f, что противоречит условию.

Система многочленов Штурма (4)

Достаточность. Если многочлен f имеет кратный корень ξ, то, в силу леммы 18.3, ξ является корнем и многочлена f'. Тогда, в силу следствия из теоремы Безу, многочлен $x - \xi$ делит и f, и f'. Следовательно, $x - \xi$ делит наибольший общий делитель многочленов f и f'. В силу п. а) это означает, что $(x - \xi) \mid f_m$. Но тогда f_m имеет действительный корень ξ вопреки условию.

в) Если многочлены $f_0 = f$ и $f_1 = f'$ имеют общий действительный корень, то, в силу леммы 18.3, этот корень является кратным корнем многочлена f. Следовательно, f_0 и f_1 не имеют общих действительных корней. Из равенства $f_0 = q_1 f_1 - f_2$ вытекает, что если бы многочлены f_1 и f_2 имели общий корень, то этот корень был бы и корнем многочлена f_0. Следовательно, он был бы общим корнем многочленов f_0 и f_1, что противоречит сказанному выше. Таким образом, f_1 и f_2 общих корней не имеют. Аналогично, из равенства $f_1 = q_2 f_2 - f_3$ и отсутствия общих корней у многочленов f_1 и f_2 вытекает их отсутствие у многочленов f_2 и f_3. Продолжая эти рассуждения, мы в конце концов докажем, что общие корни отсутствуют у многочленов f_i и f_{i+1} для всякого $i = 0, 1, \ldots, m - 1$.

Система многочленов Штурма (5)

г) Если $f_k(\xi) = 0$ для некоторого $\xi \in \mathbb{R}$ и некоторого $0 < k < m$, то, полагая $x = \xi$ в равенстве $f_{k-1}(x) = q_k(x)f_k(x) - f_{k+1}(x)$, мы получаем, что $f_{k-1}(\xi) = q_k(\xi) \cdot 0 - f_{k+1}(\xi) = -f_{k+1}(\xi)$. При этом $f_{k-1}(\xi), f_{k+1}(\xi) \neq 0$ в силу п. в). Следовательно, числа $f_{k-1}(\xi)$ и $f_{k+1}(\xi)$ равны по модулю и имеют противоположные знаки. $\square$

Теорема Штурма (1)

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_k$ — произвольный упорядоченный набор ненулевых действительных чисел. *Переменой знака* в этом наборе чисел будем называть ситуацию, когда, для некоторого $1 \leqslant i \leqslant k-1$, числа α_i и α_{i+1} имеют разные знаки.

Пусть $f(x) \in \mathbb{R}[x]$, $f_0, f_1, \ldots, f_m$ — система многочленов Штурма для многочлена f, а ξ — произвольное действительное число. Рассмотрим упорядоченный набор чисел $f_0(\xi), f_1(\xi), \ldots, f_m(\xi)$. Вычеркнем из него все нули. Обозначим через $W(\xi)$ число перемен знака в оставшемся наборе чисел.

Теорема 18.4 (теорема Штурма)

Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$, не имеющий кратных корней, а $f_0, f_1, \ldots, f_m$ — система многочленов Штурма для многочлена f. Пусть, далее, $a, b \in \mathbb{R}$, $a < b$ и числа a и b не являются корнями многочлена $f(x)$. Тогда $W(a) \geqslant W(b)$ и число корней многочлена $f(x)$ в отрезке $[a, b]$ равно $W(a) - W(b)$.

Теорема Штурма (2)

Доказательство. Как и в доказательстве предложения 18.3, мы будем пользоваться непрерывностью многочленов над $\mathbb{R}$ как функций из $\mathbb{R}$ в $\mathbb{R}$.

Посмотрим, как меняется число $W(x)$, когда x движется, возрастая, от a к b. Предположим сначала, что ни один из многочленов f_0, f_1, …, f_m при этом ни разу не меняет знак. Ясно, что в этом случае $W(a) = W(b)$. С другой стороны, в этом случае многочлен $f_0 = f$ сохраняет знак в интервале (a, b). Кроме того, в этом интервале сохраняет знак многочлен $f_1 = f'$, а это значит, что f является монотонной функцией на (a, b). Ясно, что в этом случае f не имеет корней в интервале (a, b). Таким образом, как число корней многочлена $f(x)$ в отрезке $[a, b]$, так и число $W(a) - W(b)$ равны 0. В частности, они равны между собой.

Предположим теперь, что при движении x от a к b по крайней мере один из многочленов f_0, f_1, …, f_m хотя бы один раз изменил знак. Ясно, что если многочлен f_i изменил знак при переходе x через точку $\xi \in (a, b)$, то ξ — корень многочлена f_i.

Теорема Штурма (3)

Число корней многочлена конечно, и потому число точек интервала (a, b), в которых меняется знак хотя бы одного из многочленов f_0, f_1, …, f_m, тоже конечно. Обозначим эти точки через $c_1, c_2, \ldots, c_s$ и будем считать без ограничения общности, что $c_1 < c_2 < \cdots < c_s$. Кроме того, для удобства обозначений, положим $c_0 = a$ и $c_{s+1} = b$.

Пока x проходит любой из интервалов (c_i, c_{i+1}), где $i = 0, 1, \ldots, s$, знаки многочленов f_0, f_1, …, f_m, а значит, и число перемен знаков в последовательности чисел $f_0(x)$, $f_1(x)$, …, $f_m(x)$ не меняются. Посмотрим, как меняется число перемен знаков в этой последовательности, когда x проходит через точку c_k для некоторого $1 \leqslant k \leqslant s$. В силу выбора точек $c_1, c_2, \ldots, c_s$, при переходе x через c_k по крайней мере один из многочленов f_0, f_1, …, f_m меняет знак. Пусть f_i, где $0 \leqslant i \leqslant m$, — произвольный многочлен, изменивший знак при переходе x через c_k. В частности, это означает, что $f_i(c_k) = 0$. Согласно п. б) леммы 18.4, $i < m$. Дальнейшие рассмотрения распадаются на два случая.

Случай 1: $i > 0$. Из п. в) леммы 18.4 вытекает, что числа $f_{i-1}(c_k)$ и $f_{i+1}(c_k)$ отличны от 0. Следовательно, существует $\varepsilon > 0$ такое, что каждый из многочленов f_{i-1} и f_{i+1} сохраняет знак в интервале $(c_k - \varepsilon, c_k + \varepsilon)$, а многочлен f_i сохраняет знак в каждом из интервалов $(c_k - \varepsilon, c_k)$ и $(c_k, c_k + \varepsilon)$.

Теорема Штурма (4)

В силу п. г) леммы 18.4, знаки многочленов f_{i-1} и f_{i+1} в интервале $(c_k - \varepsilon, c_k + \varepsilon)$ различны. Предположим сначала, что $f_i(x) > 0$ при $x \in (c_k - \varepsilon, c_k)$ и $f_i(x) < 0$ при $x \in (c_k, c_k + \varepsilon)$. Если $f_{i-1}(x) > 0$ и $f_{i+1}(x) < 0$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, то имеет место ситуация, указанная в строках 1 и 2 табл. 1, а если $f_{i-1}(x) < 0$ и $f_{i+1}(x) > 0$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, — ситуация, указанная в строках 3 и 4 той же таблицы (табл. 1 расположена на следующем слайде; во всех строках этой таблицы, как и в табл. 2 ниже, красным цветом указаны ситуации, в которых возникает перемена знака). Если же $f_i(x) < 0$ при $x \in (c_k - \varepsilon, c_k)$ и $f_i(x) > 0$ при $x \in (c_k, c_k + \varepsilon)$, то, в зависимости от знаков чисел $f_{i-1}(x)$ и $f_{i+1}(x)$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, имеет место ситуация, указанная либо в строках 5 и 6 табл. 1, либо в строках 7 и 8 этой таблицы.

Мы видим, что если в интервале $(c_k - \varepsilon, c_k)$ перемена знака в последовательности чисел $f_0(x)$, $f_1(x)$, ..., $f_m(x)$ происходила при переходе от многочлена f_i к f_{i+1}, то в интервале $(c_k, c_k + \varepsilon)$ она будет происходить при переходе от f_{i-1} к f_i (см. строки 1, 2, 7 и 8 табл. 1). И наоборот, если в интервале $(c_k - \varepsilon, c_k)$ перемена знака происходила при переходе от f_{i-1} к f_i, то в интервале $(c_k, c_k + \varepsilon)$ она будет происходить при переходе от f_i к f_{i+1} (см. строки 3–6 табл. 1).

Теорема Штурма (5)

Таким образом, за счет того, что многочлен f_i при $0 < i < m$ меняет знак в точке c_k, перемена знака в последовательности чисел $f_0(x)$, $f_1(x)$, ..., $f_m(x)$ может «сдвинуться на одну позицию» влево или вправо, но число перемен знаков в этой последовательности измениться не может.

Табл. 1. Перемена знака «сдвигается»

	x принадлежит интервалу	$f_{i-1}(x)$	$f_i(x)$	$f_{i+1}(x)$
1	$(c_k - \varepsilon, c_k)$	> 0	> 0	< 0
2	$(c_k, c_k + \varepsilon)$	> 0	< 0	< 0
3	$(c_k - \varepsilon, c_k)$	< 0	> 0	> 0
4	$(c_k, c_k + \varepsilon)$	< 0	< 0	> 0
5	$(c_k - \varepsilon, c_k)$	> 0	< 0	< 0
6	$(c_k, c_k + \varepsilon)$	> 0	> 0	< 0
7	$(c_k - \varepsilon, c_k)$	< 0	< 0	> 0
8	$(c_k, c_k + \varepsilon)$	< 0	> 0	> 0

Теорема Штурма (6)

Случай 2: $i = 0$. Это означает, что c_k — корень многочлена f_0. Из п. в) леммы 18.4 вытекает, что c_k не является корнем многочлена f_1. Следовательно, существует $\varepsilon > 0$ такое, что многочлен f_1 сохраняет знак в интервале $(c_k - \varepsilon, c_k + \varepsilon)$, а многочлен f_0 сохраняет знак в каждом из интервалов $(c_k - \varepsilon, c_k)$ и $(c_k, c_k + \varepsilon)$. Напомним, что $f = f_0$ и $f_1 = f'$. Если $f_1(\xi) > 0$ для всех $\xi \in (c_k - \varepsilon, c_k + \varepsilon)$, то многочлен $f = f_0$ монотонно возрастает в интервале $(c_k - \varepsilon, c_k + \varepsilon)$, и потому $f_0(\xi) < 0$ при $\xi \in (c_k - \varepsilon, c_k)$ и $f_0(\xi) > 0$ при $\xi \in (c_k, c_k + \varepsilon)$. Если же $f_1(\xi) < 0$ для всех $\xi \in (c_k - \varepsilon, c_k + \varepsilon)$, то многочлен $f = f_0$ монотонно убывает в интервале $(c_k - \varepsilon, c_k + \varepsilon)$, и потому $f_0(\xi) > 0$ при $\xi \in (c_k - \varepsilon, c_k)$ и $f_0(\xi) < 0$ при $\xi \in (c_k, c_k + \varepsilon)$. Таким образом, имеет место ситуация, указанная либо в строках 1 и 2 табл. 2, либо в строках 3 и 4 той же таблицы (см. следующий слайд).

Мы видим, что знаки чисел $f_0(x)$ и $f_1(x)$ различаются в интервале $(c_k - \varepsilon, c_k)$ и совпадают в интервале $(c_k, c_k + \varepsilon)$. Иными словами, в интервале $(c_k - \varepsilon, c_k)$ в последовательности чисел $f_0(x)$, $f_1(x)$, $\ldots$, $f_m(x)$ происходит перемена знака при переходе от многочлена f_0 к f_1, а в интервале $(c_k, c_k + \varepsilon)$ эта перемена знака отсутствует. Таким образом, за счет того, что многочлен f_0 меняет знак в точке c_k, число перемен знаков в последовательности чисел $f_0(x)$, $f_1(x)$, $\ldots$, $f_m(x)$ уменьшается на 1.

Теорема Штурма (7)

Табл. 2. Перемена знака исчезает

	x принадлежит интервалу	$f_0(x)$	$f_1(x)$
1	$(c_k - \varepsilon, c_k)$	< 0	> 0
2	$(c_k, c_k + \varepsilon)$	> 0	> 0
3	$(c_k - \varepsilon, c_k)$	> 0	< 0
4	$(c_k, c_k + \varepsilon)$	< 0	< 0

Итак, при движении x от a к b число перемен знаков в последовательности чисел $f_0(x)$, $f_1(x)$, $\ldots$, $f_m(x)$ меняется только в случае, когда x проходит через точку, в которой многочлен $f_0 = f$ меняет знак, причем в этом случае оно уменьшается на 1. Следовательно, разность $W(a) - W(b)$ равна числу таких точек. Ясно, все числа, при переходе через которые многочлен f меняет знак, являются его корнями.

Теорема Штурма (8)

Осталось проверить, что других корней у многочлена f на интервале (a, b) нет. В самом деле, пусть ξ — корень многочлена f, принадлежащий интервалу (a, b), и этот многочлен при переходе x через ξ не меняет знак. В силу следствия из теоремы Безу, $f(x) = (x - \xi)g(x)$ для некоторого многочлена $g(x)$. Ясно, что двучлен $x - \xi$ меняет знак при переходе x через ξ. Поскольку $f(x)$ при этом знака не меняет, мы получаем, что многочлен $g(x)$ меняет знак при переходе x через ξ. Это означает, что число ξ является корнем многочлена $g(x)$, а значит, — корнем кратности $\geqslant 2$ многочлена $f(x)$. Но по условию многочлен f не имеет кратных корней. □

Следствие о числе корней многочлена

Из теоремы Штурма и следствия 18.5 вытекает следующее утверждение.

Следствие 18.8

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен степени* > 0 *над полем* $\mathbb{R}$*, не имеющий кратных корней. Число действительных корней многочлена* $f(x)$ *равно* $W(-R_f) - W(R_f)$. □

Теорема Штурма доказана в предположении, что многочлен не имеет кратных корней. Однако ее можно использовать для нахождения числа корней произвольного многочлена над полем $\mathbb{R}$, принадлежащих заданному отрезку $[a, b]$. В самом деле, пусть f — произвольный многочлен степени > 0 над полем $\mathbb{R}$. Положим $g = \frac{f}{d}$, где d — наибольший общий делитель многочленов f и f'. В силу следствия 18.6 многочлены f и g имеют одни и те же корни, причем второй из них не имеет кратных корней. Поэтому можно применить теорему Штурма к многочлену g и найти число корней многочлена f в отрезке $[a, b]$. Аналогично, применяя следствие 18.8 к многочлену $g = \frac{f}{d}$, можно найти общее число действительных корней произвольного многочлена f.

Приближенное решение уравнений

Начав с интервала $(-R_f, R_f)$ и последовательно уменьшая размеры интервалов (например, методом половинного деления) и применяя к каждому из полученных интервалов теорему Штурма, можно для каждого корня многочлена $f \in \mathbb{R}[x]$ найти интервал числовой прямой, содержащий этот корень и не содержащий никаких других корней. Продолжая процесс половинного деления, можно сделать интервалы, содержащие корни, сколь угодно маленькими. Это означает, что мы можем приближенно найти все действительные корни многочлена f с любой наперед заданной степенью точности. Иными словами,

- *теорему Штурма можно использовать для приближенного решения алгебраических уравнений.*

18.6. Рациональные корни многочленов над полем $\mathbb{Q}$

Перейдем к вопросу о нахождении рациональных корней многочленов над полем $\mathbb{Q}$. Очевидно, что многочлен из $\mathbb{Q}[x]$ может не иметь рациональных корней даже в том случае, когда у него есть действительные корни. В качестве примера, подтверждающего этот факт, можно взять многочлен $x^2 - 2$. Оказывается, однако, что с помощью несложных вычислений можно выяснить, есть ли у данного многочлена над полем $\mathbb{Q}$ рациональные корни, и если они есть, то найти их.

Если не все коэффициенты многочлена $f \in \mathbb{Q}[x]$ являются целыми числами, можно домножить его на наименьшее общее кратное знаменателей всех дробей, являющихся его коэффициентами. Полученный многочлен будет иметь те же корни, что и f, а все его коэффициенты будут целыми числами. Поэтому далее можно рассматривать только многочлены над $\mathbb{Q}$ с целыми коэффициентами.

Предложение 18.4

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ — многочлен над полем $\mathbb{Q}$ 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.

Рациональные корни многочленов с целыми коэффициентами (2)

Доказательство. Поскольку $\frac{p}{q}$ — корень многочлена $f(x)$, имеем:

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \cdot \frac{p}{q} + a_0 = 0. \qquad (6)$$

Умножив обе части этого равенства на q^n, получим:
$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$. Отсюда получаем:
$a_0 q^n = p(-a_n p^{n-1} - a_{n-1} p^{n-2} q - \cdots - a_1 q^{n-1})$. Поэтому p делит $a_0 q^n$.
Поскольку числа p и q взаимно просты, p делит a_0. Аналогично, q делит a_n, поскольку $a_n p^n = q(-a_{n-1} p^{n-1} - \cdots - a_1 p q^{n-2} - a_0 q^{n-1})$. □

Определение

Многочлен называется *унитарным*, если его старший коэффициент равен 1.

Из предложения 18.4 непосредственно вытекает следующий факт.

Следствие 18.9

Если $f(x)$ — унитарный многочлен над полем $\mathbb{Q}$ с целыми коэффициентами, то все рациональные корни многочлена $f(x)$ являются целыми числами и делят свободный член этого многочлена. □

Рациональные корни многочленов с целыми коэффициентами (3)

Поскольку число делителей старшего коэффициента и свободного члена многочлена над полем $\mathbb{Q}$ с целыми коэффициентами конечно, предложение 18.4 сводит задачу нахождения рациональных корней таких многочленов к несложному перебору. Этот перебор можно существенно сократить, если использовать следующее утверждение (см. комментарий после его доказательства).

Предложение 18.5

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен над полем* $\mathbb{Q}$ *с целыми коэффициентами,* $\frac{p}{q}$ *— рациональное число и несократимая дробь, а* m *— произвольное целое число. Если* $\frac{p}{q}$ *— корень многочлена* $f(x)$*, то* $p - mq$ *делит* $f(m)$*.*

Рациональные корни многочленов с целыми коэффициентами (4)

Доказательство. Ясно, что

$$f(m) = a_n m^n + a_{n-1} m^{n-1} + \cdots + a_1 m + a_0.$$

Вычтем из этого равенства равенство (6). Получим:

$$f(m) = a_n\left(m^n - \left(\frac{p}{q}\right)^n\right) + a_{n-1}\left(m^{n-1} - \left(\frac{p}{q}\right)^{n-1}\right) + \cdots + a_1\left(m - \frac{p}{q}\right).$$

Умножив это равенство на q^n, получим

$$q^n f(m) = a_n(m^n q^n - p^n) + a_{n-1} q(m^{n-1} q^{n-1} - p^{n-1}) + \cdots + a_1 q^{n-1}(mq - p). \quad (7)$$

Учитывая, что для любого целого s и для любых $a, b \in \mathbb{R}$ выполнено равенство $a^s - b^s = (a-b)(a^{s-1} + a^{s-2}b + \cdots + ab^{s-2} + b^{s-1})$, получаем, что $mq - p$ делит $m^s q^s - p^s$ для всех $s = 2, 3, \ldots, n$. Из равенства (7) вытекает теперь, что $mq - p$ делит $q^n f(m)$. Проверим, что $mq - p$ взаимно просто с q^n. Предположим, что это не так. Тогда существует простое число r, которое делит и $mq - p$, и q^n. Из того, что r — простое число и r делит q^n, вытекает, что r делит q. Учитывая, что r делит еще и $mq - p$, получаем, что r делит p. Но r не может одновременно делить и p, и q, поскольку числа p и q взаимно просты. Итак, $mq - p$ делит $q^n f(m)$ и взаимно просто с q^n. Следовательно, $mq - p$ делит $f(m)$.

Рациональные корни многочленов с целыми коэффициентами (комментарий)

Предложение 18.5 позволяет существенно сократить перебор делителей старшего коэффициента и свободного члена многочлена с целыми коэффициентами при поиске его рациональных корней, поскольку оно показывает, что (в обозначениях предложений 18.4 и 18.5) можно рассматривать только такие пары (p, q), что $p - q$ делит $f(1)$, $p + q$ делит $f(-1)$, $p - 2q$ делит $f(2)$ и т. д.

Отметим еще, что, поскольку $f(0) = a_0$, предложение 18.5 обобщает утверждение предложения 18.4 о том, что p делит a_0.