Корни уравнений с целыми коэффициентами

М.Д. Малых, РУДН

8 ноября 2022 г.

Содержание

Дифференцирования колец
 Комплексные нули многочленов с целыми коэффициентами
 Поле алгебраических чисел
 Что значит решить уравнение?
 Задания

1. Дифференцирования колец

Исследование кратностей корней уравнений тесно связано с понятием дифференцирования.

Определение 1. Правило T, по которому элементам множества A ставятся элементы множества B, называют отображением A в B, пишут $T:A\to B$.

Определение 2. Отображение T кольца A в кольцо B называют линейным, если

$$T(a+b) = T(a) + T(b).$$

Определение 3. Линейное отображение D кольца A в кольцо A называют дифференцированием, если выполняется правило Лейбница

$$D(ab) = a \cdot D(b) + D(a) \cdot b.$$

Образ элемента a, то есть Da, называют производной a. Элементы кольца A, которые переходят в нуль кольца A, называют константами относительно дифференцирования D.

Чтобы определить дифференцирование кольца многочленов k[x], введем новую переменную dx и для любого $f \in k[x]$ рассмотрим выражение

$$f(x + dx) = f(x) + f_1(x)dx + f_2(x)dx^2 + \dots$$

как элемент кольца k[x][dx]. Коэффициент при dx является некоторым многочленом из k[x]. Определим отображение D как сопоставление многочлену $f \in k[x]$ коэффициента при dx в выражении $f(x+dx) \in k[x][dx]$:

$$Df = [f(x+dx)]_{dx}.$$

Это отображение является линейным, поскольку для любых двух многочленов f и g верно

$$D(f+g) = [f(x+dx)+g(x+dx)]_{dx} = [f(x+dx)]_{dx} + [g(x+dx)]_{dx} = D(f) + D(g).$$

Поскольку выполняется правило Лейбница:

$$D(fg) = [f(x+dx)g(x+dx)]_{dx} =$$

$$= [(f(x) + f_1(x)dx + \dots) \cdot (g(x) + g_1(x)dx + \dots)]_{dx} =$$

$$= [f(x)g(x) + f_1(x)g(x)dx + f(x)g_1(x)dx + \dots)]_{dx} = fDg + gDf,$$

это отображение действительно является дифференцированием кольца k[x]. Для многочлена f нулевой степени, то есть элемента поля k, верно

$$f(x + dx) = f(x),$$

поэтому производная многочлена нулевой степени равна нулю. Если степень многочлена больше нуля, то его производная не является нулем k[x].

Таким образом, нули дифференцирования D образуют множество, которое совпадает с полем k.

Если многочлен $f \in k[x]$ приведен к нормальной форме, то

$$D(a_n x^n + \dots + a_1 x + a_0) = n a_n x^{n-1} + \dots + a_1.$$

Отсюда сразу видно, что производная многочлена с рациональными коэффициентами не зависит от того, рассматриваем ли мы дифференцирование над \mathbb{Q} , \mathbb{R} или \mathbb{C} .

B Sage имеется функция diff, при помощи которой можно дифференцировать любые символьные выражения.

Пример 1. sage: var("x")

2. Комплексные нули многочленов с целыми коэффициентами

Пусть f и g — два многочлена из $\mathbb{Q}[x]$. Поскольку в этом кольца всякий идеал — главный,

$$(f,g) = (r)$$

Теорема 1. Множество комплексных корней, общих для f и g, совпадает с множеством нулей многочлена r.

Доказательство. Допустим, что $x=a\in\mathbb{C}$ — комплексный корень, общий для f и g, то есть f(a)=g(a)=0. Тогда из $r\in(f,g)$ следует, что существуют такие многочлены $u,v\in\mathbb{Q}[x]$, что

$$uf + vg = r$$

и поэтому r(a) = u(a)f(a) + v(a)g(a) = 0.

Обратно, допустим, что $x=a\in\mathbb{C}$ — комплексный корень r, то есть r(a)=0. Тогда из $f,g\in(r)$ следует, что существуют такие многочлены $u,v\in\mathbb{Q}[x]$, что

$$f = ur$$
, $q = vr$

и поэтому
$$f(a) = u(a)r(a) = 0$$
 и $g(a) = v(a)r(a) = 0$.

Эта теорема имеет одно весьма важно следствие.

Теорема 2. Если f, g — простые многочлены кольца $\mathbb{Q}[x]$, то они не имеют общих комплексных корней.

Доказательство. Если f, g — простые многочлены кольца $\mathbb{Q}[x]$, то (f, g) = 1. Уравнение 1 = 0 не имеет корней, следовательно, совместных корней не имеют и многочлены f, g.

Допустим, что многочлен $f \in \mathbb{Q}[x]$ имеет комплексный корень x=a кратности m, тогда

$$f = (x - a)^m g,$$

где $g \in \mathbb{C}[x]$ и $g(a) \neq 0$. В таком случае,

$$Df = m(x-a)^{m-1}g + (x-a)^m Dg = (x-a)^{m-1}(mg + (x-a)Dg).$$

Множитель mg + (x-a)Dg при x=a равен $mg(a) \neq 0$, поэтому производная имеет нуль кратности m-1.

Теорема 3. Все комплексные нули простого многочлена кольца $\mathbb{Q}[x]$ имеют кратность 1.

Доказательство. Допустим, что простой многочлен f имеет комплексный нуль x=a кратности m>1, тогда многочлены f и Df имеют совместный нуль x=a. Но тогда (f,Df)=(r) и степень r больше 1. Из $Df\in (r)$ следует, что степень r строго меньше степени f, а из $f\in (r)$ следует, что f делится на r, что невозможно.

Пример 2. Какой бы простой многочлен мы не взяли, его комплексные корни — простые.

Разложим многочлен $f \in \mathbb{Q}[x]$ на простые множители

$$f = C p_1^{m_1} \dots p_r^{m_r}$$

В силу теоремы 3 все корни p_i — простые, а в силу теоремы 2 среди корней простых сомножителей нет повторяющихся. Поэтому корни многочлена p_1 будут корнями исходного многочлена кратности m_1 , корни p_2 — корнями кратности m_2 и т.д. Это означает, что кратности комплексных корней совпадают с крайностями разложения многочлена над \mathbb{Q} . Именно по этой причине в Sage кратности комплексных корней определяются точно, а сами значения корней — приближенно.

3. Поле алгебраических чисел

Определение 4. Комплексное число α называется алгебраическим, если оно является корнем некоторого многочлена из $\mathbb{Z}[x]$.

Множество всех алгебраических чисел обозначается как $\overline{\mathbb{Q}}$ (QQbar), множество всех вещественных алгебраических чисел — как \mathbb{A} (AA).

Если алгебраическое число α является корнем некоторого многочлена из $\mathbb{Q}[x]$, то оно является корнем и некоторого его простого множителя. В силу теоремы 2 не существует другого простого многочлена, корнем которого было бы это число. Поэтому многочлен минимальной степени, корнем которого является заданное алгебраическое число, определен однозначно с точность до мультипликативной константы.

Определение 5. Многочлен наименьшей степени из $\mathbb{Z}[x]$, корнем которого является алгебраическое число, называется минимальным многочленом этого числа.

Пример 3. sage: alpha=sqrt(2)
sage: QQbar(alpha)
1.414213562373095?
18
sage: QQbar(alpha).minpoly()
19
x^2 - 2

Теорема 4. Сумма и произведение двух алгебраических чисел является алгебраическим числом.

 $\ensuremath{\mathcal{A}\!o\kappa a}$ зате
мельство. Пусть α и β — два алгебраических числа.

Рассмотрим комплексное число $\gamma=\alpha+\beta$. Его степень всегда можно раскрыть

$$\gamma^s = \alpha^s + \dots + \beta^s,$$

то есть представить как линейную комбинацию выражений вида

$$\alpha^{s_1}\beta^{s_2}, \quad (s_1 + s_2 = s)$$

над \mathbb{Z} . Если степень минимального многочлена для α равна m, то

$$a_m \alpha^m + \dots + a_0 = 0, \quad a_i \in \mathbb{Z},$$

и поэтому любую степень α , начиная с α^m , можно представить как линейную комбинацию

$$1, \alpha, \dots, \alpha^{m-1}$$

над \mathbb{Q} . Аналогично, если n- степень минимального многочлена для β , то любую его степень можно представить как как линейную комбинацию

$$1, \beta, \ldots, \beta^{n-1}$$

над \mathbb{Q} . Но тогда, сколь бы ни было велико s, число γ^s можно представить как линейную комбинацию выражений вида

$$\alpha^{s_1} \beta^{s_2}, \quad (s_1 < m, \, s_2 < n)$$

Всего таких выражений mn. Расположим их в каком-то порядке, перенумеруем от 1 до nm и будем обозначать далее как $\varphi_1, \ldots, \varphi_{nm}$. В таком случае, комплексные числа γ^s при любом натуральном значении s можно представить как линейную комбинацию nm чисел $\varphi_1, \ldots, \varphi_{nm}$ над \mathbb{Q} :

$$\gamma^s = \sum_{p=1}^{nm} a_{sp} \varphi_p,$$

где $a_{sp} \in \mathbb{Q}$.

Посмотрим теперь на систему из mn+1 линейного уравнения

$$\sum_{p=1}^{nm} a_{sp} x_p = b_s \quad (s = 0, \dots, nm)$$

из $\mathbb{C}[x_1,\ldots,x_{mn}]$. Уравнений здесь больше, чем неизвестных, поэтому решение существует не при любой правой части. Применяя метод Гаусса, мы придем на некотором шаге к соотношению вида

$$c_0 b_0 + c_1 b_1 + \dots + c_r b_r = 0,$$

где c_0, \ldots, c_r — рациональные числа. При $b_s = \gamma^s$ эта система линейных уравнений разрешима, поэтому

$$c_0 + c_1 \gamma + \dots + c_r \gamma^r = 0,$$

то есть число γ должно быть корнем уравнения r-ой степени.

Аналогично доказывается, что произведение $\alpha\beta$ является алгебраическим числом.

Доказательство теоремы дает конструктивный путь к отысканию минимального многочлена для суммы и произведения двух алгебраических чисел.

Пример 4. Рассмотрим сумму двух алгебраических чисел, скажем, $\gamma = \sqrt{2} + \sqrt{3}$. Оба слагаемых — корни квадратного уравнения (n = m = 2), поэтому γ^s выражается через $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, напр.,

$$\begin{cases} \gamma = \sqrt{2} + \sqrt{3} \\ \gamma^2 = 2\sqrt{6} + 5 \\ \gamma^3 = 9\sqrt{3} + 11\sqrt{2} \\ \gamma^4 = 20\sqrt{6} + 49 \\ \gamma^5 = 89\sqrt{3} + 109\sqrt{2} \end{cases}$$

Поэтому система линейных уравнений

$$\begin{cases} \gamma = x_1 + x_2 \\ \gamma^2 = 2x_3 + 5x_0 \\ \gamma^3 = 9x_2 + 11x_1 \\ \gamma^4 = 20x_3 + 49x_0 \\ \gamma^5 = 89x_2 + 109x_1 \end{cases}$$

разрешима. В данном случае, она распадается на две не связанные подсистемы. Рассмотрим первую из них:

$$\begin{cases} \gamma = x_1 + x_2 \\ \gamma^3 = 9x_2 + 11x_1 \\ \gamma^5 = 89x_2 + 109x_1 \end{cases}$$

Исключим x_1 из второго и третьего уравнений:

$$\begin{cases} \gamma = x_1 + x_2 \\ \gamma^3 - 11\gamma = -2x_2 \\ \gamma^5 - 109\gamma = -20x_2 \end{cases}$$

Исключая x_2 из последнего уравнения, найдем

$$\begin{cases} \gamma = x_1 + x_2 \\ \gamma^3 - 11\gamma = -2x_2 \\ \gamma^5 - 109\gamma - 10(\gamma^3 - 11\gamma) = 0 \end{cases}$$

Таким образом, γ — корень уравнения

$$\gamma^5 - 10\gamma^3 + \gamma = 0.$$

Поскольку рассматриваемая сумма отлична от нуля, $\sqrt{2} + \sqrt{3}$ — корень уравнения

$$\gamma^4 - 10\gamma^2 + 1 = 0.$$

Sage знает, что сумма и произведение алгебраических чисел— алгебраическое число и может найти его минимальный многочлен.

Пример 5. sage: alpha=QQbar(sqrt(2))

$$x^4 - 10*x^2 + 1$$

$$x^2 - 6$$

Теорема 5. Множество всех алгебраических чисел $\overline{\mathbb{Q}}$ является полем.

 \mathcal{A} оказательство. Поскольку арифметические операции не выводят за множество $\overline{\mathbb{Q}}$, а само это множество вложено в поле комплексных чисел \mathbb{C} , то множество $\overline{\mathbb{Q}}$ является кольцом. Обратный для элемента α , являющегося корнем уравнения

$$a_n x^n + \dots + a_0 = 0, \quad a_i \in \mathbb{Z}$$

будет комплексное число $\beta=1/\alpha,$ которое удовлетворяет уравнению

$$a_n + \dots + a_0 x^n = 0, \quad a_i \in \mathbb{Z}$$

то есть тоже алгебраическое число. Поэтому кольцо $\overline{\mathbb{Q}}$ является полем. \square

Теорема 6. Множество всех вещественных алгебраических чисел A является полем.

Sage эти теоремы известны:

4. Что значит решить уравнение?

Задача об отыскании корней уравнения n-ой степени с целыми коэффициентами

$$a_n x^n + \dots + a_0 = 0$$

была сформулирована еще на заре появления алгебры. Подытожим, что в системе Sage можно сделать с такими уравнениями.

Прежде всего многочлен f с целыми коэффициентами можно разложить на простые множители в кольце $\mathbb{Q}[x]$:

$$a_n x^n + \dots + a_0 = a_n p_1^{m_1} \dots p_r^{m_r}.$$

Уравнение имеет рациональные корни в том и только в том случае, если среди простых множителей p_1, \ldots, p_r имеются линейные. Более того, только линейные множители имеют рациональные корни. Таким образом, задача об отыскании рациональных корней заданного уравнения с целыми коэффициентами полностью решена.

Пример 6. Найдем все рациональные корни уравнения

$$4x^6 - 128x^5 + 129x^4 - 155x^3 - 3x^2 + 94x - 31 = 0$$

Разложим его на простые множители над $\mathbb Z$ или $\mathbb Q$:

Отсюда сразу видно, что у него два рациональных корня — x=1/2 и x=31.

Если же мы желаем найти корни в \mathbb{R} или \mathbb{C} , то следует решить, в каком виде мы хотим их представить. Мы можем найти приближенно все вещественные корни и точно указать их кратности.

Пример 7. Найдем все вещественные корни уравнения

$$4x^6 - 128x^5 + 129x^4 - 155x^3 - 3x^2 + 94x - 31 = 0$$

Разложим его на простые множители над \mathbb{RR} :

```
sage: RR[x](4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 3* 33
    x^2 + 94*x - 31).factor()

(4.0000000000000) * (x - 31.0000000000) * (x - 34
    0.5000000000000)^2 * (x + 0.682327803828019) * (
    x^2 - 0.682327803828019*x + 1.46557123187677)
```

Отсюда сразу видно, что у него три вещественных корня: два рациональных и еще один вещественный корень простого многочлена $x^3+x+1\in\mathbb{Z}[x]$. Мы можем в Sage задать a как этот корень:

```
sage: ZZ[x](4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 3* 35
    x^2 + 94*x - 31).roots(RR)
[(-0.682327803828019, 1), (0.500000000000000, 2), 36
    (31.000000000000, 1)]
sage: a=ZZ[x](4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 37
    3*x^2 + 94*x - 31).roots(RR)[0][0]
```

Дальше мы можем оперировать с этим числом, но при этом нужно помнить об ошибке округления:

Реализация полей \mathbb{A} и $\overline{\mathbb{Q}}$ в Sage, позволяет сохранить вместе с корнем его минимальный многочлен, что позволяет проводить вычисления точно. Эта реализация позволяет балансировать на гране между алгеброй и приближенными вычислениями.

Пример 8. Найдем все вещественные корни уравнения

$$4x^6 - 128x^5 + 129x^4 - 155x^3 - 3x^2 + 94x - 31 = 0$$

в поле \mathbb{A} . В разложим на простые множители над \mathbb{A} мы получим то же выражение, что и над \mathbb{R} :

Как и раньше, что у него три вещественных корня: два рациональных и еще один вещественный корень простого многочлена $x^3 + x + 1 \in \mathbb{Z}[x]$. Мы можем в Sage задать a как этот корень:

```
sage: ZZ[x](4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 3* 42
    x^2 + 94*x - 31).roots(AA)

[(-0.6823278038280193?, 1), (0.500000000000000000?, 43
    2), (31.0000000000000?, 1)]

sage: a=ZZ[x](4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 44
    3*x^2 + 94*x - 31).roots(AA)[0][0]
```

Как и в \mathbb{RR} подстановка в уравнение этого корня не дает точный нуль:

sage:
$$(4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 3*x^2 + 45$$

 $94*x - 31).subs(x=a)$
0.?e-35

Однако это число — алгебраическое и мы можем вычислить его минимальный многочлен:

sage:
$$(4*x^6 - 128*x^5 + 129*x^4 - 155*x^3 - 3*x^2 + 47$$

 $94*x - 31).subs(x=a).minpoly()$

48

Корнем этого уравнения является x=0, то есть при подстановке в уравнение корня мы получаем точный нуль.

Х

Алгебраисты былых времен стремились получить корни в конечном виде. Вероятно, Паоло Руффини (Paolo Ruffini; 1765—1822) был первым, кто сформулировал, что именно это значит. Мы хотим представить корень уравнение в виде символьного выражения, сторожащего целые числа и арифметические операции. Если ограничить множество арифметических операций 4-мя действиями, то такие выражения являются рациональными числами. Искать рациональные корни мы умеем. Если же добавить к ним операцию извлечения корня, получаются алгебраические числа, среди которых точно есть иррациональные, напр., $\sqrt{2}$.

Под решением алгебраического уравнения подразумевают отыскание выражений для его корней, содержащих целые числа, соединенные арифметическими действиями, включая извлечение корня. Все ли корни алгебраического уравнения с целыми коэффициентами можно представить в таком виде? Всякое ли алгебраическое число можно представить в таком виде? — Ответ на этот вопрос — отрицательный, а его обоснование составляет содержание теории Галуа.

Однако в ряде частных случаев такое представление отыскать удается, в том числе для всех уравнений 3-й и 4-й степени. В ряде случаев найти такое выражение можно в Sage, используя замечательный метод

radical_expression.

Пример 9. Найдем выражения в радикалах для всех вещественных корней уравнения

$$4x^6 - 128x^5 + 129x^4 - 155x^3 - 3x^2 + 94x - 31 = 0$$

Практическая польза представления корней в виде радикалов в настоящее время представляется спорной. В прошлые века в ходу были методы извлечения корня в столбик¹, поэтому отыскание такого рода выражений в радикалах сводило приближенное вычисление корней алгебраического уравнения к расчетам на бумаге. Однако теперь в нашем распоряжении есть прямые методы приближенного вычисления корней алгебраического уравнения и часто решение в поле А более удобно для работы, чем огромное выражение в радикалах. Однако возможность такого представления чрезвычайно полезна при решении разного рода учебных задач, ответ в которых желают получить именно в такой форме.

Пример 10. Найдите все точки минимума функции

$$y = x(x-1)(x-2)(x-3).$$

 $^{^1}$ Шрейдер С.Н. Алгебра. Рабочая книга для подготовки в ВУЗ. 3-е изд. М.: Работник Просвещения, 1930.

Разумеется, задача рассматривается на вещественной прямой, поэтому мы будем работать над A. Как известно, точки экстремума — корни уравнения

$$D(x(x-1)(x-2)(x-3)) = 0.$$

Находим эти корни:

Там, где вторая проводная больше нуля, имеется минимум, где меньше нуля—максимум. Проверим, что вторая производная в стационарных точках не равна нулю.

Точки минимума:

Таким образом, мы имеем две точки миниммума. При желании, мы можем выразить ее в радикалах:

Однако далеко не всегда ответ выглядит столь кратко и понятно.

Пример 11. Найдите все точки максимума функции

$$y = x(x-1)(x-2)(x-4).$$

Точки экстремума — корни уравнения

$$D(x(x-1)(x-2)(x-4)) = 0.$$

Находим эти корни:

Проверим, что вторая производная в стационарных точках не равна нулю.

Теперь, не боясь, оставляем в списке только те точки, где вторая производная меньше нуля:

Таким образом, мы имеем единственную точку максимума. При желании, мы можем выразить ее в радикалах:

```
sage: [a.radical_expression() for a in R if diff(y,x 73
    ,2).subs(x=a)<0]
[-1/2*(5/72*I*sqrt(23)*sqrt(3) + 15/64)^(1/3)*(I* 74
    sqrt(3) + 1) - 35/96*(-I*sqrt(3) + 1)/(5/72*I*sqrt
    (23)*sqrt(3) + 15/64)^(1/3) + 7/4]</pre>
```

Появившаяся здесь мнимая единица не противоречит нашему определению, ведь ее можно заменить на $\sqrt{-1}$. Само число — вещественное, но представление в радикалах содержит содержит i. Это не только удивительно, но и весьма трудно для дальнейшего использования. Напр., Sage не может конвертировать это выражение в вещественное число и выдает ошибку «unable to convert '1.53090655551522+1.11022302462516e-16*I' to a real number» при конвертировании в элемент RR или «unable to convert 5/72*I to an element of Algebraic Real Field» при конвертировании в элемент AA.

5. Задания

Теоретические вопросы.

- 1) Что такое дифференцирование кольца k[x]?
- 2) Может ли простой многочлен с целыми коэффициентами иметь кратные корни?
- 3) Могут ли простые многочлены с целыми коэффициентами иметь общие корни?
- 4) Что такое иррациональное число? Что такое алгебраическое число?
- Дайте определения минимального многочлена алгебраического числа.
 Практические задания.
 - 1) Найдите первую и вторую производную функции $x^3(x-2)^2$.
 - 2) Найдите минимальный многочлен алгебраического числа $\sqrt{2+\sqrt[3]{5}}$.
 - 3) Найдите рациональные корни многочленов: а.) $x^4 9x^3 + 25x^2 27x + 10$, b.) $4x^5 24x^4 + 13x^3 + 43x^2 42x + 10$.
 - 4) Найдите вещественные корни многочленов и выразите их в радикалах: a.) $x^3 + x + 1$, b.) $4x^5 - 24x^4 + 13x^3 + 43x^2 - 42x + 10$, c.) $4x^6 - 24x^5 + 25x^4 - 21x^3 - 27x^2 + 37x - 10$.

- 5) Найдите комплексные корни многочленов и выразите их в радикалах: а.) x^3+x+1 , b.) $4x^5-24x^4+13x^3+43x^2-42x+10$, c.) $4x^6-24x^5+25x^4-21x^3-27x^2+37x-10$.
- 6) Найдите точки минимума функции $y = (x^2 1)(x + 3)(x 2)$.
- 7) Найдите точки максимума функции $y = \frac{x^3-2}{x^2+1}$.
- 8) Найдите наименьшее значение функции $y = x^6 x^2 + x$ на отрезке [-1,1]. Ответ выразите в радикалах.