Системы алгебраических уравнений

М.Д. Малых, РУДН

1 декабря 2022 г.

Содержание

1. Системы алгебраических уравнений

Пусть k — некоторое поле, напр., $\mathbb{Q}$ и пусть $f_1, \dots f_m$ — m многочленов из кольца $k[x_1, \dots, x_n]$. Эти многочлены задают систему алгебраических уравнений

$$f_1 = 0, \dots, f_m = 0$$

относительно неизвестных $x_1, \dots x_n$. Пусть k вложено в некоторое поле K.

Определение 1. Точка $(a_1, \dots, a_n) \in K^n$ называется решением системы

$$f_1 = 0, \dots, f_m = 0,$$

если

$$f_1(a_1, \dots, a_n) = 0, \dots, f_m(a_1, \dots, a_n) = 0.$$

Множество всех решений системы S из K^n будем называть алгебраическим многообразием (variety) и обозначать как $\mathrm{Sol}(S, K)$.

В теории линейных уравнений мы говорили, что две системы эквивалентны друг другу, если совпадают их множества решений. В случае нелинейных уравнений это соглашение кажется весьма неудобным, поскольку множества решений одной и той же системы S зависят от выбора K.

Пример 1.

$$S_1: \quad x^3 - x^2 + 4x - 4 = 0$$

и

$$S_1: \quad x = 1$$

имеют одно и то же множество решений над $\mathbb{Q}$:

$$\mathrm{Sol}(S_1, \mathbb{Q}) = \mathrm{Sol}(S_2, \mathbb{Q}) = \{x = 1\},$$

но различные множества над $\mathbb{C}$:

$$\mathrm{Sol}(S_1, \mathbb{C}) \neq \mathrm{Sol}(S_2, \mathbb{C}) = \{x = 1\}.$$

Говорить, что S_1 и S_2 эквивалентны над $\mathbb{Q}$ не принято.

Чтобы отделить понятие эквивалентности от поля, в котором ищется решение, заметим следующее.

Теорема 1. Пусть J — идеал кольца $k[x_1, \ldots, x_n]$, порожденный многочленами $f_1, \ldots, f_m$ системы S, и $a \in \mathrm{Sol}(S, K)$. Тогда для любого $g \in J$ верно

$$g(a) = 0.$$

Доказательство. Для любого $g \in J$ найдутся такие $g_i \in k[x_1, \ldots, x_n]$, что

$$g = g_1 f_1 + \cdots + g_m f_m.$$

Поэтому на $a \in \mathrm{Sol}(S, K)$ верно

$$g(a) = g_1(a) f_1(a) + \cdots + g_m(a) f_m(a) = 0.$$

□

Доказанная теорема позволяет считать многочлены идеала $J = (f_1, \ldots, f_m)$ — следствиями уравнений исходной системы S. Поэтому обычно говорят не о решении системы S, а об алгебраическим множестве, порожденном идеалом.

Определение 2. Пусть J — идеал кольца $k[x_1, \ldots, x_n]$ Алгебраическое многообразие $Z(J, K)$ образовано точками $(a_1, \ldots, a_n) \in K^n$, которые являются нулями всех многочленов из J.

В идеал попадают не все следствия, поэтому вынужденно вводят понятие радикала идеала.

Пример 2. Рассмотрим уравнение

$$(x-1)^2 = 0$$

В идеал J, порожденный многочленом $(x-1)^2$, попадают не все многочлены, равные нулю в точке $x = 1$, но только имеющие в этой точке кратность 2 и более.

Определение 3. Радикал $\sqrt{J}$ из идеала J кольца A — это множество всех элементов кольца A, для каждого их которых, скажем, для f, можно найти такое натуральное число r, что

$$f^r \in J.$$

В Sage имеется возможность вычислять радикалы из идеалов в кольце $\mathbb{Q}[x_1, \ldots, x_n]$. При этом используется весьма сложный алгоритм, обсуждение которого выходит за рамки настоящего курса.

Пример 3.

```
sage: var("x,y")
(x, y)                                                    2
sage: A=QQ[x,y]                                           3
sage: J=A*[(x+y)^2, (x-y)^3]                              4
sage: J                                                   5
```

```
Ideal (x^2 + 2*x*y + y^2, x^3 - 3*x^2*y + 3*x*y^2 -
  y^3) of Multivariate Polynomial Ring in x, y over
  Rational Field
sage: J.radical()
Ideal (y, x) of Multivariate Polynomial Ring in x, y
   over Rational Field
```

Таким образом, вместо понятия следствия системы уравнений, мы будем говорить об идеале J, порожденной системой уравнений, и о его радикале $\sqrt{J}$.

2. Исключение неизвестных

Что значит найти x_i из системы алгебраических уравнений, порождающих идеал J кольца $\mathbb{Q}[x_1, \ldots, x_n]$? — Мы едва ли сможем найти явные выражения для возможных комплексных значений x_i, поскольку даже в одномерном случае нам это не удалось. Однако мы можем составить уравнение, которому удовлетворяет x_i.

Задача 1. Дан идеал J кольца $k[x_1, \ldots, x_n]$. Требуется найти множество

$$J \cap k[x_i].$$

Множество

$$J \cap k[x_i]$$

само является идеалом, его называют исключительным идеалом.

Определение 4. Пусть J — идеал кольца $k[x_1, \ldots, x_n]$, тогда множество

$$J \cap k[x_{i_1}, \ldots, x_{x_s}]$$

называют исключительным идеалом (elimination ideal), полученным путем исключения x_j, где $j \neq i_1, \ldots, i_s$.

Для решения поставленной задачи нам нужно некоторое обобщение метода Гаусса на нелинейный случай. Таковое было предложено относительно недавно, в 1930-е годы, Грёбнером.

Определение 5. Конечное множество многочленов $g_1, \ldots, g_p$ идеала J кольца $k[x_1, \ldots, x_n]$, называется базисом Гребнера этого идеала, если

1) $J = (g_1, \ldots, g_p)$,

2) $\mathrm{lm}(g_1) > \mathrm{lm}(g_2) > \cdots > \mathrm{lm}(g_p)$,

3) для любого $f \in J$ найдется такое i, что $\mathrm{lm}(f)$ делится на $\mathrm{lm}(g_i)$.

Алгоритм построения базисов Гребнера был предложен его учеником Бухбергером, его реализация открыла возможность решать системы нелинейных уравнений на компьютере.

Пример 4.
```
sage: A=PolynomialRing(QQ,[x,y],order='lex')
sage: J=A*[x-y^2,x^2-y]
sage: J.groebner_basis()
[x - y^2, y^4 - y]
sage: J=A*[x-y^2,x^3+x*y-y,y*x]
sage: J.groebner_basis()
[x, y]
```

Теорема 2. Пусть $(g_1, \ldots, g_p)$ — базис Гребнера идеала J кольца $k[x_1, \ldots, x_n]$, на мономах котором используется lex-порядок. Тогда или последний элемент базиса Гребнера принадлежит $k[x_n]$ и порождает исключительный идеал

$$J \cap k[x_n],$$

или этот идеал пуст.

Доказательство. При lex-порядке степень x_n всегда меньше любого монома, содержащего $x_1, \ldots, x_{n-1}$. Поэтому многочлен, старший член которого

является степенью x_n, принадлежит $k[x_n]$. Иными словами, $lm(f)$ является степенью x_n тогда и только тогда, когда $f \in k[x_n]$.

Пусть g_p не принадлежит $k[x_n]$, тогда его старший моном не является степенью x_n, и тем более старшие мономы остальных базисных элементов. Допустим, что при этом

$$J \cap k[x_n] \neq \emptyset.$$

Тогда имеется такой $g \in J$, что $\mathrm{lm}(g)$ является степенью x_n, которая не может делиться на старшие мономы базисных элементов, что противоречит п. 3. определения базиса Гребнера. Поэтому в этом случае пересечение пусто.

Пусть g_p принадлежит $k[x_n]$, тогда

$$g_p \in J \cap k[x_n],$$

поэтому исключительный идеал не пуст. Этот идеал — идеал кольца главных идеалов, поэтому имеется такой многочлен $h \in k[x_n]$, что

$$J \cap k[x_n] = (h).$$

Но из $g_p \in (h)$ следует, что g_p делится на h, а из $\mathrm{lm}(h)$ делится на $\mathrm{lm}(g_i) > \mathrm{lm}(g_p)$ следует, что степень h не меньше, чем степень g_p. Поэтому g_p и h отличаются лишь на константу из поля k и

$$J \cap k[x_n] = (g_p).$$

□

Пример 5.

```
sage: J=A*[x-y^2,x^3+x*y-y]
sage: J.groebner_basis()
[x - y^2, y^6 + y^3 - y]
sage: J.elimination_ideal([A(x)])
Ideal (y^6 + y^3 - y) of Multivariate Polynomial
  Ring in x, y over Rational Field
```

3. Конечные многообразия

Если уравнений достаточно много, то определяемое ими многообразие является конечным множеством. Исключая все переменные, кроме одной, мы можем отыскать все решения такой системы.

Пример 6. Рассмотрим систему

$$x - y^2 + 2 = 0, \quad x^2 y = 1$$

```
sage: S=[x-y^2+2,x^2*y-1]
sage: J=A*S
sage: J.groebner_basis()
[x - y^2 + 2, y^5 - 4*y^3 + 4*y - 1]
sage: T=J.groebner_basis()
sage: yy=ZZ[y](T[1]).roots(QQbar)
```

Таким образом, y может принимать одно из 5 указанных значений. Переберем их по очереди. Для первого имеем:

```
sage: y0=yy[0][0]
sage: T[0].subs(y=y0)
x + 1.927561975482926?
sage: QQbar[x](T[0].subs(y=y0)).roots()
[(-1.927561975482926?, 1)]
sage: x0=QQbar[x](T[0].subs(y=y0)).roots()[0][0]
sage: x0
-1.927561975482926?
sage: [s.subs(x=x0).subs(y=y0) for s in S]
[0.?e-38, 0.?e-37]
```

Для второго:

```
sage: y1=yy[1][0]
```

```
sage: T[0].subs(y=y0)
x + 1.927561975482926?
sage: QQbar[x](T[0].subs(y=y1)).roots()
[(-1, 1)]
sage: x1=QQbar[x](T[0].subs(y=y1)).roots()[0][0]
sage: x1
-1
sage: [s.subs(x=x1).subs(y=y1) for s in S]
[0, 0]
```

Таким путем мы найдем 5 точек.

В Sage эта процедура автоматизирована при помощи метода `variety(K)`, который применяется к идеалу.

Пример 7. Рассмотрим опять систему

$$x - y^2 + 2 = 0, \quad x^2 y = 1$$

```
sage: S=[x-y^2+2,x^2*y-1]
sage: J=A*S
sage: J.variety(QQbar)
[{y: 1, x: -1}, {y: 0.2691431301688280?, x:
  -1.927561975482926?}, {y: 1.665774328417699?, x:
  0.7748041132154347?}, {y: -1.467458729293264? -
  0.2775899692806873?*I, x: 0.07637893113374587? +
  0.8147036471703865?*I}, {y: -1.467458729293264? +
  0.2775899692806873?*I, x: 0.07637893113374587? -
  0.8147036471703865?*I}]
sage: J.variety(QQ)
[{y: 1, x: -1}]
```

Точки многообразия возвращаются в форме словаря (dictionary, стандартный питоновский тип):

```
sage: J.variety(QQ)[0]['x']
-1
```

4. Задания

Теоретические вопросы.

1) Дайте определение алгебраического многообразия.

2) Дайте определение радикала из идеала.

3) Дайте определение базиса Гребнера.

4) Как найти пересечение $J \cap k[x_1]$, если имеется возможность вычислить базис Гребнера идеала J?

Практические задания.

1) Дана система уравнений

$$x^2 + y^2 - z^2 = 0,\ x - 2y^2 - 3,\ z + x - y - 3 = 0$$

Найдите все точки, удовлетворяющие системе уравнений, из a.) $\mathbb{Q}^3$, b.) $\mathbb{R}^3$ и c.) $\mathbb{C}^3$.

2) Вычислите радикал идеала

$$J = ((x+y)^2 + (x-z)^2 + 1,\ (x+y)^4 + (x-z)^4 + z,\ 2x + y - z)$$

Совпадают ли идеала J и $\sqrt{J}$? Совпадают ли многообразия, порожденные J и $\sqrt{J}$?

3) На плоскости $\mathbb{R}^2$ найдите координаты точек пересечения кривой

$$x^3 - y^3 = 2xy$$

и окружности $x^2 + y^2 = 1$. Ответ выразите в радикалах.

4) Составьте уравнение, которому удовлетворяют z-координаты точек многообразия

$$x^2 + y^2 = z^3,\ x - 2y^2 = 3,\ z + x - y = 3.$$

Является ли это уравнение простым в $\mathbb{Q}[z]$?

5) Найдите уравнение проекции линии

$$x^2 + y^2 + z^2 = 2, \quad x^2 + z^2 = 1$$

на плоскость xy.

6) Определите размерность многообразия

$$x^2 - y^2 + xz - yz = 0,\ x + y + z = 0,\ x = y.$$

7) Укажите, сколько точек пересечения может иметь парабола $y = x^2$ и прямая $y = kx + b$ при различных значениях k и b.

8) Опишите множество точек пересечения поверхности

$$x^2 + y^2 = z^2$$

и плоскости

$$(x - 1) + (y - 1) = \sqrt{2}(z - \sqrt{2}),$$

касающейся этой поверхности в точке $(1, 1, \sqrt{2})$.