Кольцо многочленов

М.Д. Малых, РУДН

28 августа 2022 г.

Содержание

1. Многочлены и кольцо многочленов

Пусть A — некоторое кольцо.

Определение 1. Выражение, составленное из элементов этого кольца, букв $x_1, \dots, x_n$ и символов сложения и умножения, называют многочленом от переменных $x_1, \dots, x_n$ над кольцом A.

Замечание. При этом, конечно, предполагают, что подстановка элементов $a_1, \dots a_n$ кольца A на место переменных $x_1, \dots, x_n$ дает некоторый элемент кольца A, именуемый значением многочлена в точке $(a_1, \dots, a_n)$. Напр., выражение $(x_1 + 2x_2)x_2$ или `(x1+2*x2)*x2` мы многочленом считаем, а выражение `x1*8*` — нет.

Замечание. К числу разрешенных действий (сложение и умножение) мы в дальнейшем будем добавлять вычитание и возведение в натуральную степень. Напр., выражение $(x_1 - x_2)^2$ содержит возведение в степень и вычитание, но его можно переписать как $(x_1 + (-1) \cdot x_2) \cdot (x_1 + (-1) \cdot x_2)$ при помощи только двух разрешенных действий.

Теорема 1. Множество всех многочленов от переменных $x_1, \dots, x_n$ над кольцом A является кольцом.

Определение 2. Множество всех многочленов от переменных $x_1, \dots, x_n$ над кольцом A является называется кольцом многочленов и обозначается как $A[x_1, \dots, x_n]$

В Sage в качестве обозначения для переменных можно использовать любые наборы буквы, при желании к буквам можно добавлять цифры, но только справа. Для задания многочлена от некоторых переменных прежде всего нужно указать их имена, после чего можно вводить сам многочлен:

```
sage: var("x,y")
(x, y)
sage: (x-y)^3
(x - y)^3
```

Для колец многочленов используется обозначение, введенное в определение 2:

```
sage: QQ[x]
Univariate Polynomial Ring in x over Rational Field
sage: QQ[x,y]
```

```
Multivariate Polynomial Ring in x, y over Rational
   Field
```

При этом

```
sage: (x-y)^3 in QQ[x]
False
sage: (x-y)^3 in QQ[x,y]
True
```

В некоторых случаях бывает удобно использовать более длинную форму записи:

```
sage: PolynomialRing(QQ,[x,y])
Multivariate Polynomial Ring in x, y over Rational
   Field
sage: PolynomialRing(QQ,[x,y])==QQ[x,y]
True
```

2. Нормальная форма многочлена

Определение 3. Элементы полиномиального кольца $A[x_1, \ldots, x_n]$, представляющие собой произведение переменных $x_1, \ldots, x_n$ называют мономами.

Определение 4. Пусть выражения $y_1, \ldots y_r$ можно складывать и умножать на элементы кольца A, тогда выражение

$$a_1 y_1 + \cdots + a_r y_r, \quad a_1, \ldots, a_r \in A,$$

называют линейной комбинацией $y_1, \ldots y_r$ над кольцом A, а $a_1, \ldots, a_r$ — ее коэффициентами.

Теорема 2. Всякий многочлен кольца $A[x_1, \ldots, x_n]$ можно представить как линейную комбинацию конечного числа мономов над кольцом A.

Для получения такого представления достаточно раскрыть скобки.

Теорема 3. Представление многочлена в виде линейной комбинации мономов определено с точностью до перестановки слагаемых и отбрасывания слагаемых с нулевыми коэффициентами.

Определение 5. Представление многочлена в виде линейной комбинации мономов с ненулевыми коэффициентами называют нормальной формой многочлена.

В Sage символьное выражение как элемент того или иного полиномиального кольца описывается своим нормальным представлением.

```
sage: (x-2*y)^3+x*y^3 in QQ[x,y]
True
sage: QQ[x,y]((x-2*y)^3+x*y^3)
x*y^3 + x^3 - 6*x^2*y + 12*x*y^2 - 8*y^3
```

При необходимости можно получить списки входящих в многочлен мономов и коэффициентов при них:

```
sage: QQ[x,y]((x-2*y)^3+x*y^3).monomials()
[x*y^3, x^3, x^2*y, x*y^2, y^3]
sage: QQ[x,y]((x-2*y)^3+x*y^3).coefficients()
[1, 1, -6, 12, -8]
```

Замечание. В случае кольца $\mathbb{Q}[x, y]$ нормальную форму можно получить, раскрыв скобки:

```
sage: expand((x-2*y)^3+x*y^3)
x*y^3 + x^3 - 6*x^2*y + 12*x*y^2 - 8*y^3
```

3. Степень многочлена

Список всех мономов, которые входят в нормальное представление многочлена f с ненулевыми коэффициентами, будем обозначать как $M(f)$, а список этих коэффициентов, взятых в том же порядке, как $C(f)$. В Sage предусмотрена возможность вывести эти списки .

Пример 1. Многочлен $(x-2y)^3 + xy^3$ кольца $\mathbb{Q}[x,y]$ имеет следующую нормальную форму

```
sage: f=((x-2*y)^3+x*y^3)
sage: QQ[x,y](f)
x*y^3 + x^3 - 6*x^2*y + 12*x*y^2 - 8*y^3
```

Вот список входящих в нее мономов:

```
sage: QQ[x,y](f).monomials()
[x*y^3, x^3, x^2*y, x*y^2, y^3]
```

Вот список коэффициентов, с которыми эти мономы входят в нормальное представление

```
sage: QQ[x,y](f).coefficients()
[1, 1, -6, 12, -8]
```

Разумеется, по этим двум спискам всегда можно восстановить нормальное представление многочлена:

```
sage: C=QQ[x,y](f).coefficients()
sage: M=QQ[x,y](f).monomials()
sage: sum([C[n]*M[n] for n in range(len(M)) ])
x*y^3 + x^3 - 6*x^2*y + 12*x*y^2 - 8*y^3
```

Определение 6. Степенью монома

$$x_1^{k_1} \dots x_n^{k_n}$$

называют число

$$\mathrm{degree}(x_1^{k_1} \dots x_n^{k_n}) = k_1 + \dots + k_n.$$

Степенью многочлена f называют максимальную из степеней мономов, входящих в $m(f)$. Степень многочлена p обозначают как $\mathrm{degree}(p)$.

Пример 2. Вот список мономов, входящих в нормальное представление многочлена $(x-2y)^3 + xy^3$ кольца $\mathbb{Q}[x,y]$:

```
sage: f=((x-2*y)^3+x*y^3)
sage: QQ[x,y](f).monomials()
[x*y^3, x^3, x^2*y, x*y^2, y^3]
```

Вот список их степеней

```
sage: M = QQ[x,y](f).monomials()
sage: [QQ[x,y](m).degree() for m in M]
[4, 3, 3, 3, 3]
```

Хорошо видно, что максимальное значение равно 4. Но это можно получить и в Sage:

```
sage: max([QQ[x,y](m).degree() for m in M])
4
```

Разумеется, степень можно вычислить и прямо:

```
sage: QQ[x,y](f).degree()
4
```

4. Мономиальный порядок

Чтобы устранить неопределенность в порядке следования слагаемых в нормальной форме, вводят порядок на множестве мономов.

Определение 7. Линейным порядком (linear order) на множестве M называют бинарное отношение $\leq$, определенное для любых двух элементов этого множества и удовлетворяющее следующим условиям. Для любых $a, b, c \in M$ верно

1) $a \leq a$ (рефлексивность);

2) $a \leq b$ и $b \leq c$ влечет $a \leq c$ (транзитивность);

3) $a \leq b$ и $b \leq a$ влечет $a = b$ (антисимметричность).

Множество, на котором задан линейный порядок, называется линейно упорядоченным. Если $a \neq b$ и $a \leq b$, то пишут $a < b$.

Напр., сравнение больше-меньше в поле $\mathbb{R}$ является линейным порядком.

Определение 8. Мономиальный порядок (monomial order) — линейный порядок на множестве M мономов полиномиального кольца, удовлетворяющий условиям. Для любых $u, v, w \in M$ верно

1) $u \leq v$ влечет $uw \leq vw$;

2) $1 \leq u$.

Мономиальный порядок можно вводить несколькими способами.

Определение 9. Лексикографический порядок (lexicographic order, lex) на множестве мономов кольца $A[x_1, \ldots, x_n]$ — это линейный порядок, при котором

$$x_1^{k_1} \ldots x_n^{k_n} > x_1^{l_1} \ldots x_n^{l_n}$$

означает, что существует такой номер i, что

$$k_1 = l_1, \ldots, k_{i-1} = l_{i-1},\ k_i > l_i.$$

Определение 10. Градуированный лексикографический порядок (degree lexicographic order, deglex) на множестве мономов кольца $A[x_1, \ldots, x_n]$ — это мономиальный порядок, при котором

$$x_1^{k_1} \ldots x_n^{k_n} > x_1^{l_1} \ldots x_n^{l_n}$$

означает, что

$$k_1 + \cdots + k_n > l_1 + \cdots + l_n$$

или

$$k_1 + \cdots + k_n = l_1 + \cdots + l_n$$

и существует такой номер i, что

$$k_1 = l_1, \ldots, k_{i-1} = l_{i-1},\ k_i > l_i.$$

Для явного указания порядка на мономах в функции PolynomialRing предусмотрена опция order.

```
sage: A=PolynomialRing(QQ,[x,y], order='lex')
sage: B=PolynomialRing(QQ,[x,y], order='deglex')
sage: A(x^2*y)>A(x*y^3)
True
sage: B(x^2*y)>B(x*y^3)
False
```

Поясним этот результат. При lex-порядке важно, что степень первой переменной (т.е. x) для монома x^2y равна 2, а для монома xy^3 равна 1, поэтому

$$x^2y > xy^3.$$

При lex-порядке важно, что степень монома x^2y равна 3, а степень монома xy^3 равна 4, поэтому

$$x^2y < xy^3.$$

Рассмотрим более сложный пример.

```
sage: var('z')
z
sage: C=PolynomialRing(QQ,[x,y,z], order='lex')
sage: C(x*y^2*z^2) >C(x*y*z^5)
True
```

В обоих рассматриваемых мономах степени при первой переменной совпадают, а степени при второй переменной различны и $2 > 1$, что дает $xy^2z^p > xyz^q$ и степени z не важны.

По умолчанию в Sage используют именно deglex-порядок на множестве мономов, а слагаемые в нормальной форме многочлена всегда располагают по старшинству, начиная со старшего монома.

```
sage: A((x^2*y+x*y^3)^2)
x^4*y^2 + 2*x^3*y^4 + x^2*y^6
```

```
sage: B((x^2*y+x*y^3)^2)
x^2*y^6 + 2*x^3*y^4 + x^4*y^2
```

Этот же порядок сохраняется в списках мономов и коэффициентов многочлена.

```
sage: A((x^2*y+x*y^3)^2).monomials()
[x^4*y^2, x^3*y^4, x^2*y^6]
sage: B((x^2*y+x*y^3)^2).monomials()
[x^2*y^6, x^3*y^4, x^4*y^2]
```

Кольца $\mathbb{QQ}[x, y]$ и $\mathbb{QQ}[y, x]$ совпадают с точностью до выбора мономиального порядка. Первой считается не x, а та переменная, которая указана первой в списке переменных.

```
sage: QQ[x,y](x)>QQ[x,y](y)
True
sage: QQ[y,x](x)>QQ[y,x](y)
False
```

Определение 11. Старшим членом (leading term) многочлена называют первый член в его нормальной форме, этот член представляет собой произведение старшего коэффициента на старший моном.

В Sage имеются функции для их отыскания:

```
sage: A((x^2*y+x*y^3)^2).lt()
x^4*y^2
sage: A((x^2*y+x*y^3)^2).lm()
x^4*y^2
sage: A((x^2*y+x*y^3)^2).lc()
1
```

5. Различия в реализации полиномиальных колец с одной и несколькими неизвестными

В Sage полиномиальных колец с одной и несколькими неизвестными реализованы по разному. Выше мы рассматривали примеры с несколькими неизвестными. В случае кольца с одной неизвестной вместо функции `monomials` используется `exponents`.

```
sage: QQ[x]
Univariate Polynomial Ring in x over Rational Field
sage: QQ[x,y]
Multivariate Polynomial Ring in x, y over Rational Field
sage: QQ[x](x^3+x+2)
x^3 + x + 2
sage: QQ[x,y](x^3+x+2)
x^3 + x + 2
sage: QQ[x](x^3+x+2).coefficients()
[2, 1, 1]
sage: QQ[x,y](x^3+x+2).coefficients()
[1, 1, 2]
sage: QQ[x](x^3+x+2).exponents()
[0, 1, 3]
sage: QQ[x,y](x^3+x+2).exponents()
[(3, 0), (1, 0), (0, 0)]
sage: QQ[x,y](x^3+x+2).monomials()
[x^3, x, 1]
```

6. Вычисление значения многочлена в точке

В Sage мы можем найти значение многочлена несколькими способами, так или иначе использующими метод `subs` (подстановка, substitution). Если мы рассматриваем многочлен над $\mathbb{Z}$ и хотим вычислить его значение в точке с рациональными координатами, то мы можем работать с символьным выражением:

```
sage: var("x,y")
(x, y)
sage: (x+2*y+3).subs(x=1/2).subs(y=2/3)
29/6
sage: (x+2*y+3).subs([x==1/2,y==2/3])
29/6
```

Однако можно работать с многочленом как с элементом соответствующего кольца многочленов:

```
sage:  ZZ[x,y](x+2*y+3).subs(x=1/2).subs(y=2/3)
29/6
```

При этом система считает, что переменные, на место которых что-то можно подставлять, в кольце перенумерованы, начиная с 0. Поэтому поддерживается и вот такой вариант:

```
sage:  ZZ[x,y](x+2*y+3).subs({0:1/2,1:2/3})
29/6
```

Он удобен при написании своего кода. Разумеется, подставлять можно любые символьные выражения, результатом будет символьное выражение.

В Sage здесь проявляется ряд нюансов, связанных с различиями синтаксиса при работе с кольцом символьных выражений, кольцом многочленов с одной переменной и кольцом многочленов со многими переменными. Конструкция вида `.subs(x=a)` поддерживается всегда

```
sage: (x+2*y+3).subs(x=1/2).subs(y=2/3)
29/6
sage: ZZ[x,y](x+2*y+3).subs(x=1/2).subs(y=2/3)
29/6
sage: ZZ[x](x+2*x^3+3).subs(x=1/2)
15/4
```

Списки поддерживаются при подстановке в символьные выражения, словари — в многочлены со многими переменными. При необходимости, любой многочлен всегда можно преобразовать в символьное выражение

```
sage: f=ZZ[x,y](x+2*y^2+3)
sage: type(f)
<class 'sage.rings.polynomial.
  multi_polynomial_libsingular.
  MPolynomial_libsingular'>
sage: SR(f).subs([x==1])
2*y^2 + 4
```

В старых руководствах по программированию можно встретить указание на то, что перед вычислением значения многочлена его нужно привести к специальному виду, иначе «программа не будет работать». Делать этого, разумеется, не надо. Во-первых, современные системы сделают это сами без ведома пользователя. Во-вторых, многочлен, приведенный к специальному виду, системой будет переведен обратно в нормальную форму.

Пример 3. В курсе Анализа будет показано, что $\sin x$ можно с хорошей точностью заменить многочленом Тейлора. При вычислении этого многочлена в точке $x = 1$ проблем не возникает:

```
sage: taylor(sin(x),(x,0),10)
1/362880*x^9 - 1/5040*x^7 + 1/120*x^5 - 1/6*x^3 + x
sage: RR(QQ[x](taylor(sin(x),(x,0),10^2)).subs(x=1))
0.841470984807897
```

```
sage: RR(RR[x](taylor(sin(x),(x,0),10^2)).subs(x=1))
0.841470984807897
sage: RR((taylor(sin(x),(x,0),10^2)).subs(x=1))
0.841470984807897
sage: RR(sin(1))
0.841470984807897
```

Если при вычислениях работать с многочленами как элементами кольца многочленов, то на каждом шаге выражение будет приводится к нормальному виду. Если же работать с многочленами как символьными выражениями, будут проводится лишь простейшие упрощения. Поэтому во втором случае результат получится быстрее, но он будет чрезвычайно раздут.

7. Задания

Теоретические вопросы.

1) Дайте определение нормальной формы многочлена.
2) Дайте определение степени многочлена.
3) Дайте определение линейного порядка и мономиального порядка.
4) Опишите лексикографический порядок на мономах.
5) Опишите градуированный лексикографический порядок на мономах.
6) Дайте определение старшего члена.

Практические вопросы.

1) Найдите степень многочлена $x(x+y)(x^2+y^2)$ кольца $\mathbb{Z}[x,y]$.
2) Составьте список всех мономов, входящих в многочлен $x(x+y)(x^2+y^2)$ кольца $\mathbb{Z}[x,y]$.

3) Составьте список всех мономов, входящих в многочлен $x(x+2)(x^2+3)$ кольца $\mathbb{Z}[x]$.

4) Сравните мономы xyz^3 и xy^2z при лексикографическом и градуированном лексикографическом порядках на мономах.

5) Найдите нормальную форму многочлена $(x + 2y - 3z)^3$ при лексикографическом и градуированном лексикографическом порядках на мономах. Чем они отличаются?

6) Найдите главный член многочлена $(x + 2y - 3z)^3$ при лексикографическом порядке на мономах.

7) Найдите главный коэффициент многочлена $(x + 2y - 3z)^4$ при градуированном лексикографическом порядке на мономах.

8) Многочлен $(x + y)^2 + x^2y^5$ можно рассматривать не только как элемент кольца $\mathbb{Q}[x, y]$, но и как элемент кольца $\mathbb{Q}[x][y]$, то есть кольца всех многочленов от y над кольцом $\mathbb{Q}[x]$. Найдите нормальные формы многочлена $(x + 2y - 3z)^3$ как элемента колец $\mathbb{Q}[x, y]$, $\mathbb{Q}[x, y][z]$ и $\mathbb{Q}[y, z][x]$. В каком случае главный коэффициент не будет рациональным числом?

9) Вычислите значение многочлена $x^2(x-y)$ при $x = 1/2, y = 2/3$. Какие из приведенных ниже конструкций можно использовать?

   а) `(x^2*(x-y)).subs(x=1/2).subs(y=2/3)`

   б) `(x^2*(x-y)).subs(x==1/2).subs(y==2/3)`

   в) `(x^2*(x-y)).subs([x=1/2, y=2/3])`

   г) `(x^2*(x-y)).subs([x==1/2, y==2/3])`

   д) `(x^2*(x-y)).subs({0:1/2, 1:2/3})`

   е) `(x^2*(x-y)).subs({x:1/2, y:2/3})`

   ж) `QQ[x,y](x^2*(x-y)).subs(x=1/2).subs(y=2/3)` з) `QQ[x,y](x^2*(x-y)).subs(x==1/2).subs(y==2/3)`

и) `QQ[x,y](x^2*(x-y)).subs([x=1/2, y=2/3])`

к) `QQ[x,y](x^2*(x-y)).subs([x==1/2, y==2/3])`

л) `QQ[x,y](x^2*(x-y)).subs({0:1/2, 1:2/3})`

м) `QQ[x,y](x^2*(x-y)).subs({x:1/2, y:2/3})`

10) Вычислите значение многочлена $x^2(x-3)$ при $x = 1/2$. Какие из приведенных ниже конструкций можно использовать?

а) `QQ[x](x^2*(x-3)).subs(x=1/2)`

б) `QQ[x](x^2*(x-3)).subs(x==1/2)`

в) `QQ[x](x^2*(x-3)).subs([x=1/2])`

г) `QQ[x](x^2*(x-3)).subs([x==1/2])`

д) `QQ[x](x^2*(x-3)).subs({0:1/2})`

е) `QQ[x](x^2*(x-3)).subs({x:1/2})`