Общая алгебра

М.Д. Малых

2 сентября 2021 г.

Оглавление

Глава 1.

Кольца и поля

1.1. Определения

Определение 1. Кольцо (ring) — множество A, на котором заданы две бинарные операции, называемые сложение $(+)$ и умножение $(\cdot)$, со следующими свойствами, выполняющимися для любых $a, b, c \in A$:

1) $a + b = b + a$ (коммутативность сложения);

2) $a \cdot b = b \cdot a$ (коммутативность умножения);

3) $a + (b + c) = (a + b) + c$ (ассоциативность сложения);

4) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность умножения);

5) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ и $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (дистрибутивность);

6) существует такой элемент $0 \in A$, что $a + 0 = 0 + a = a$ (существование нуля);

7) существует такой элемент $1 \in A$, что $a \cdot 1 = 1 \cdot a = a$ (существование единицы);

8) для любого $a \in A$ существует такой элемент $b \in A$, что $a + b = b + a = 0$ (существование противоположного элемента относительно сложения).

Замечание. Иногда понятие кольца трактуют шире, отказавшись от коммутативность умножения и существования единицы. Ниже под кольцом подразумевается коммутативное кольцо с единицей или явно оговорено противное.

Определение 2. Поле (field) — кольцо K, обладающее дополнительным свойством: для любого его элемента $a \neq 0$ существует такой элемент $b \in K$, что $ab = ba = 1$.

Базовые примеры:

1) Множество натуральных чисел $\mathbb{N}$ не является кольцом, поскольку не содержит 0.

2) Множество целых чисел $\mathbb{Z}$ является кольцом, но не является полем.

3) Множество рациональных чисел $\mathbb{Q}$ является полем.

4) Множество вещественных чисел $\mathbb{R}$ является полем.

1.1.1. Единственность нуля

Пусть A — кольцо, его элемент θ называют нулем, если для любого $a \in A$ верно $a + \theta = \theta + a = a$. К сожалению, верно и

$$0 + \theta = 0,$$

поскольку θ — нуль кольца, и

$$0 + \theta = \theta,$$

поскольку 0 — нуль кольца. Таким образом, все нули кольца равны друг другу. Это очень досадно, поскольку в противном случае можно было бы рассматривать нули как бесконечно малые числа и дать алгебраическое изложение математическому анализу.

1.2. Целые и рациональные числа в Sage

Sage — система компьютерной алгебры, в качестве внешнего языка используется Python, к которому добавлено множество новых функций и классов.

```
sage: NN
Non negative integer semiring
sage: ZZ
Integer Ring
sage: QQ
Rational Field
sage: RR
Real Field with 53 bits of precision
```

Функции `is_ring` и `is_field` позволяют проверить, являются ли множества кольцами или полями:

```
sage: ZZ.is_ring()
True
sage: ZZ.is_field()
False
sage: QQ.is_field()
True
sage: RR.is_field()
True
```

Замечание. В Python функция может применяться слева и справа через точку, причем во втором случае ее называют методом:

```
sage: QQ.is_field()
True
sage: is_field(QQ)
True
```

Обычно результаты применения идентичны. Различия могут проявиться, если функция с одним именем определена несколько раз. Напр, если мы переопределим функцию `is_field`, то при вызове этой функции слева будет взята функция из пользовательских определений, а при ее вызове как метода из определения, данного при описании того класса, которому принадлежит $\mathbb{Q}$:

```
sage: def is_field(x): return 8
sage: is_field(QQ)
8
sage: QQ.is_field()
True
```

Целые и рациональные числа, равно как и действия с ними, вводятся обычным образом:

```
sage: 1+ 2/3
5/3
```

При этом можно выяснить, считает ли система то или иное выражение элементом того или иного кольца:

```
sage: 5 in QQ
True
sage: 5 in ZZ
True
sage: 5/2 in ZZ
False
sage: 5/2 + 8 in QQ
True
sage: sqrt(2) in QQ
False
```

При этом:

```
sage: type(5)
<type 'sage.rings.integer.Integer'>
sage: type(5/2)
<type 'sage.rings.rational.Rational'>
```

```
sage: type(sqrt(5))
<type 'sage.symbolic.expression.Expression'>
sage: type(pi)
<type 'sage.symbolic.expression.Expression'>
```

Таким образом, целые числа считаются по умолчанию элементами кольца целых чисел, рациональные — поля рациональных чисел, а выражения, которые система не может упростить до рационального числа, — символьными выражениями.

1.3. Вещественные числа в Sage

Поле вещественных чисел реализовано в Sage как множество десятичных дробей, для хранения которых требуется не более 53 бит. Всякая десятичная дробь по умолчанию считается элементом $\mathbb{R}$:

```
sage: type(0.3)
<type 'sage.rings.real_mpfr.RealLiteral'>
```

Если система считает, что число или символьное выражение принадлежит $\mathbb{RR}$, то можно узнать соответствующую ему десятичную дробь:

```
sage: pi in RR
True
sage: RR(pi)
3.14159265358979
```

Однако здесь проявляется несколько тонких моментов.

1) С точки зрения синтаксиса вопрос `a in A` означает, может ли система рассматривать `a` как элемент множества `A`. Ответ False не означает, что `a` действительно не принадлежит `A`. Напр., путем значительных

усилий[1] можно доказать равенство

$$2\arctan\frac{1}{2} - \arctan\frac{1}{7} = \frac{\pi}{4}.$$

Однако, Sage не знает этого равенства и поэтому не может преобразовать выражение

$$2\arctan\frac{1}{2} - \arctan\frac{1}{7} - \frac{\pi}{4}$$

в рациональное число, о чем и сообщает:

```
sage: 2*atan(1/2) - atan(1/7) - pi/4  in QQ
False
```

При этом:

```
sage: 2*atan(1/2) - atan(1/7) - pi/4  in RR
True
sage: RR(2*atan(1/2) - atan(1/7) - pi/4)
0.000000000000000
```

2) Если система может рассматривать `a` как элемент множества `A`, то `A(a)` — представление `a` как элемента множества `A`. Напр., $\frac{1}{3}$ является бесконечной десятичной дробью $0.333\ldots$. Система может рассмотреть это число как элемент `RR`, но его представление в этом множестве будет уже конечной десятичной дробью:

```
sage: 1/3 in RR
True
sage: RR(1/3)
0.333333333333333
```

Таким образом, при переходе к реализации поля $\mathbb{R}$ в Sage делается небольшая ошибка, которую называют ошибкой округления.

[1] C. Störmer. Solution complète en nombres entiers de l'équation $m\arctan 1/x + n\arctan 1/y = k\pi/4$. // Bulletin de la S. M. F., tome 27 (1899), p. 160-170. URL: `http://www.numdam.org/item?id=BSMF_1899__27__160_1`.

3) Реализация поля $\mathbb{R}$ в Sage не является полем, результат зависит от порядка слагаемых:

```
sage: RR(10^20)+RR(1) - RR(10^20)
0.000000000000000
sage: RR(10^20)- RR(10^20) +RR(1)
1.00000000000000
```

Из-за этих особенностей в компьютерной алгебре стараются избегать использования поля $\mathbb{R}$.

1.4. Задания

Теоретические задания.

1) Дайте определение кольца.
2) Дайте определение поля.
3) Элемент e кольца A называется единицей, если $ae = ea = a$. Докажите, что $e = 1$.

Практические задания.

1) Зависит ли результат суммы от порядка слагаемых в реализации в Sage поля вещественных чисел?
2) Сложите 1 и 2/3 в Sage.
3) Преобразуйте π^2 в десятичную дробь.
4) Считает ли Sage выражение $\pi - \pi$ рациональным числом? Нулем?
5) Совпадает ли `QQ(RR(pi))` с числом π?
6) Совпадает ли `QQ(RR(1/3))` с числом $\frac{1}{3}$?
7) Как интерпретирует Sage числа, введенные с клавиатуры как `1/3` и `1.0/3`? Совпадают `1/3` и `1.0/3` как элементы поля $\mathbb{Q}$?

Глава 2.

Кольцо многочленов

2.1. Многочлены и кольцо многочленов

Пусть A — некоторое кольцо.

Определение 3. Выражение, составленное из элементов этого кольца, букв $x_1, \ldots, x_n$ и символов сложения и умножения, называют многочленом от переменных $x_1, \ldots, x_n$ над кольцом A.

Замечание. При этом, конечно, предполагают, что подстановка элементов $a_1, \ldots a_n$ кольца A на место переменных $x_1, \ldots, x_n$ дает некоторый элемент кольца A, именуемый значением многочлена в точке $(a_1, \ldots, a_n)$. 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 $x_1, \ldots, x_n$ над кольцом A является кольцом.

Определение 4. Множество всех многочленов от переменных $x_1, \ldots, x_n$ над кольцом A является называется кольцом многочленов и обозначается как $A[x_1, \ldots, x_n]$

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 4:

```
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
```

2.2. Нормальная форма многочлена

Определение 5. Элементы полиномиального кольца $A[x_1, \dots, x_n]$, представляющие собой произведение переменных $x_1, \dots, x_n$ называют мономами.

Определение 6. Пусть выражения $y_1, \dots y_r$ можно складывать и умножать на элементы кольца A, тогда выражение

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

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

Теорема 2. Всякий многочлен кольца $A[x_1, \dots, x_n]$ 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 7. 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
```

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
```

2.3. 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 8. 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
```

2.4. Мономиальный порядок

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

Определение 9. 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 10. 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 11. 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 12. 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 13. 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
```

2.5. 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]
```

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

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

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

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

5) 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 $\mathbb{Q}[x,y]$, $\mathbb{Q}[x][y]$ и $\mathbb{Q}[y][x]$. В каком случае главный коэффициент не будет рациональным числом?

Глава 3.

Поле частных

3.1. Делители нуля

Определение 14. Элемент $a \neq 0$ кольца A называют делителем нуля, если существует такой элемент $b \neq 0$, что $ab = 0$.

Определение 15. Кольцо A, в котором нет делителей нуля, называют целостным (entire ring, integral domain).

Нетрудно видеть, что $\mathbb{Z}$ — целостное кольцо, всякое поле тоже лишено делителей нуля, однако свойство отсутствия делителей нуля сознательно не прописано в определении кольца, поскольку дальше кольца с делителями нуля появится.

Теорема 4. Если кольцо A — целостное, то для любых многочленов $p, q \in A[x_1, \ldots, x_n]$ верно

$$\operatorname{lt}(p)\operatorname{lt}(q) = \operatorname{lt}(pq).$$

Доказательство. При умножении p на q, взятых в нормальной форме, мы получим сумму произведений входящих в них членов. Пусть m и m' — старшие мономы в p и q. При умножении pq получается член

$$\operatorname{lc}(p)\operatorname{lc}(q)mm',$$

который не может быть равен нулю, поскольку кольцо — целостное и, следовательно, $\operatorname{lc}(p)\operatorname{lc}(q)$ не может быть равно нулю. Не может этот член сократиться с другими. В самом деле, пусть n и n' — любые другие в p и q.

Тогда

$$m > n, \quad m' > n'$$

и поэтому в силу определения мономиального порядка

$$mm' > nm' > nn'.$$

Это означает, что при умножении pq получается член

$$\operatorname{lc}(p)\operatorname{lc}(q)mm'$$

старше члена при nn' и не может с ним сократиться. Более того, он старше любого другого члена в pq. □

Теорема 5. Если кольцо A — целостное, то кольцо $A[x_1,\ldots,x_n]$ тоже является целостным.

Доказательство. Если бы кольцо $A[x_1,\ldots,x_n]$ имело делители нуля, то имелись бы $p, q \neq 0$ такие, что

$$pq = 0$$

и в то же время

$$\operatorname{lt}(p)\operatorname{lt}(q) \neq 0,$$

что невозможно. □

3.2. Поле частных

Определение 16. Уравнение вида

$$ax = b,$$

где a, b принадлежат кольцу A и $a \neq 0$, а x — подлежащая определению неизвестная, называют линейным уравнением над кольцом A.

Можно сказать, что линейное уравнение над A задается многочленом первой степени кольца $A[x]$.

Линейное уравнение

$$ax = b$$

над полем F всегда имеет и притом единственное решение, равное $x = a^{-1}b$. В случае колец ситуация становится много сложнее. Во-первых, совсем не факт, что уравнение имеет решение в A. Напр., линейное уравнение

$$2x = 1$$

над кольцом $\mathbb{Z}$ не имеет решение в $\mathbb{Z}$. Во-вторых, пусть $x_1, x_2 \in A$ — два его решения, тогда

$$a(x_1 - x_2) = 0.$$

Отсюда следует, что $x_1 = x_2$ только в том случае, когда A — целостное кольцо.

Обычно решение уравнений с целыми коэффициентами ищут не в $\mathbb{Z}$, а в содержащем его поле рациональных чисел $\mathbb{Q}$.

Определение 17. Говорят, что кольцо A вложено в кольцо B, если

1) A является подмножеством B,

2) сумма и произведение двух элементов множества A не зависят от того, рассматриваются ли эти элементы как элементы кольца A или кольца B.

Определение 18. Поле F называют полем частных кольца (fraction field) A, если

1) кольцо A вложено в поле F,

2) всякий элемент поля является решением линейного уравнения вида

$$ax = b, \quad a, b \in A.$$

Пример 3. Кольцо $\mathbb{Z}$ вложено не только в $\mathbb{Q}$, но и в $\mathbb{Q}[t]$. Второй пункт определения 18 нужен для того, чтобы $\mathbb{Q}[x]$ не считалось полем частных $\mathbb{Z}$.

Для существования поля частных необходимо, чтобы кольцо было целостным.

Теорема 6. Если кольцо A имеет делители нуля, то для него нельзя вложить в поле.

Доказательство. Допустим, что A можно вложить в поле F, но при этом имеются делители нуля, т.е. такие ненулевые элементы $a, \in A$, что $ab = 0$. Поле F должно содержать обратный к a элемент c, то есть $ac = 1$. Но тогда $0 = abc = b$, что невозможно. □

Обращение этой теоремы требует знакомства с одной весьма общей конструкцией — отношением эквивалентности.

3.3. Отношение эквивалентности

Определение 19. Отношение эквивалентности ($\sim$) на множестве M — это бинарное отношение, для которого при любых $a, b, c \in M$ выполнены следующие условия:

1) рефлексивность: $a \sim a$;

2) симметричность: если $a \sim b$, то $b \sim a$;

3) транзитивность: если $a \sim b$ и $b \sim c$, то $a \sim c$.

Запись вида «$a \sim b$» читается как «a эквивалентно b».

Определение 20. Классом эквивалентности $[a]$ элемента $a \in X$ называется подмножество элементов, эквивалентных a; то есть,

$$[a] = \{\, x \in X \mid x \sim a \,\}.$$

Если $b \in [a]$, то $[b] = [a]$. Два класса эквивалентности или совпадают, или не имеют общих элементов.

Определение 21. Любой элемент класса $[a]$ называется представителем этого класса.

Для задания класса достаточно указать одного его представителя.

Определение 22. Классом эквивалентности $[a]$ элемента $a \in X$ называется подмножество элементов, эквивалентных a; то есть,

$$[a] = \{\, x \in X \mid x \sim a \,\}.$$

Определение 23. Фактормножество — множество всех классов эквивалентности заданного множества X по заданному отношению $\sim$, обозначается $X/\!\sim$.

3.4. Построение поля частных

Поле частных целостного кольца A, если оно существует, прежде всего является множеством. Чтобы построить поле, в котором решаются любые линейные уравнения

$$ax = b, \quad a, b \in A,\ a \neq 0,$$

достаточно рассмотреть множество, элементами которого являются такие уравнения.

Поскольку каждое уравнение задается парой элементов из кольца A, рассмотрим множество A^2 всех упорядоченных пар элементов этого кольца. Пару будем обозначать как (b, a). Тонкость в том, что два различных элемента A^2 могут соответствовать двум уравнениям, которые имеют одинаковые корни.

Теорема 7. Два линейных уравнения

$$ax = b \quad \text{и} \quad a'x = b', \quad (a, a' \neq 0)$$

над полем F имеют один тот же корень тогда и только тогда, когда

$$ab' = a'b.$$

От множества A^2 нам нужно перейти к другому множеству, в котором бы уравнениям с общим корням отвечал один элемент. С этой целью введем отношение эквивалентности так: пара (n, m) эквивалентна (n', m'), если

$$nm' = n'm.$$

Покажем, что это действительно эквивалентность:

1) рефлексивность: $(n, m) \sim (n, m)$, поскольку $nm = nm$

2) симметричность: если $(n, m) \sim (n', m')$, то $(n', m') \sim (n, m)$, поскольку из $nm' = n'm$ следует $n'm = nm'$;

3) транзитивность: если $(n, m) \sim (n', m')$ и $(n', m') \sim (n'', m'')$, то $(n, m) \sim (n'', m'')$, поскольку из $nm' = n'm$ и $n'm'' = n''m'$ следует

$$n' \cdot nm'' = n \cdot n'm'' = nn''m' = n'' \cdot nm' = n'' \cdot n'm = n' \cdot n''m,$$

то есть

$$n'(nm'' - n''m) = 0,$$

откуда, в силу отсутствия делителей нуля,

$$nm'' = n''m.$$

Класс эквивалентности $[(n, m)]$ будем кратко обозначать как $(n : m)$. В таком случае уравнениям $ax = b$, имеющим общий корень, соответствует один элемент $(b : a)$ фактормножества $\mathbb{A}^2/\sim$. Только нужно заметить, что элементу $(n : 0)$ соответствующие уравнение $0x = n$, которое не имеет решения. Удалив из фактормножества $\mathbb{A}^2/\sim$ два элемента $(1 : 0)$ и $(0 : 0)$, получим некоторое новое множество, которое мы обозначим как F.

Теорема 8. Пусть уравнение $ax = b$ над полем F имеет корень c, а $a'x = b'$ — корень c'. Тогда $c + c'$ является корнем уравнения

$$aa'x = a'b + ab',$$

а cc' — корнем уравнения

$$aa'x = bb'.$$

Введем на нем арифметические операции:

1) $(b : a) + (b' : a') = (ab' + a'b : aa')$,

2) $(b : a) \cdot (b' : a') = (bb' : aa')$.

Тогда F является полем, поскольку выполнены все аксиомы определения кольца и поля. Более того, $(0 : 1)$ является нулем, а $(1 : 1)$ — единицей. Противоположным к $(b : a)$ будем $(-b : a)$, а обратным к $(b : a) \neq (1 : 0)$ — элемент $(a : b)$. Это поле содержит A, если отождествить элемент $a \in A$ с классом $(a : 1)$.

Всякий элемент $(b : a)$ поля F является корнем уравнения

$$(a : 1)x = (b : 1)$$

или просто $ax = b$, это поле является полем частных кольца A.

Теорема 9. Для любого целостного кольца существует поле частных.

3.5. Поля частных в Sage

Функция `FractionField` позволяет задать поле частных для кольца, указанного в ее аргумента.

Для кольца $\mathbb{Z}$ имеем:

```
sage: FractionField(ZZ)
Rational Field
sage: FractionField(ZZ)==QQ
True
```

Для кольца $\mathbb{Z}[x]$ имеем:

```
sage: var("x")
x
sage: FractionField(QQ[x])
```

```
Fraction Field of Univariate Polynomial Ring in x over Rational Field
sage: 1/2*x in FractionField(QQ[x])
True
```

В Sage кольцо или поле, которому принадлежит заданный элемент, рассматривается как его родитель:

```
sage: 1/QQ[x](x)
1/x
sage: (1/QQ[x](x)).parent()
Fraction Field of Univariate Polynomial Ring in x over Rational Field
sage: (1/x).parent()
Symbolic Ring
```

3.6. Задания

Теоретические задания.

1) Дайте определение делителя нуля. Дайте определение целостного кольца.

2) Приведите примеры целостных колец.

3) Дайте определение поля частных.

4) Дайте определение отношения эквивалентности.

5) Докажите теорему 7.

6) Проверьте выполнение аксиом из определений кольца и поля для действий, введенных на множестве F на стр. 26.

Практические задания.

1) Задайте в Sage поле частных для кольца $\mathbb{Q}[x, y]$.

2) Совпадают ли поля частных колец $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$ в Sage?

3) Совпадает ли поле частных для поля $\mathbb{Q}$ с самим полем?

4) Рассматривается кольцо $\mathbb{Q}[x, y]$. Какому кольцу/полю принадлежит x/y с точки зрения Sage?

Глава 4.

Системы линейных уравнений

4.1. Определение

Пусть A — произвольное кольцо.

Определение 24. Уравнение $f = 0$, левая часть f которого является многочленом первой степени кольца $A[x_1, \dots, x_n]$, называется линейным уравнением над кольцом A с n неизвестными $x_1, \dots, x_n$ или линейным уравнением из кольца $A[x_1, \dots, x_n]$.

Более развернуто, линейное уравнение — это уравнение вида

$$a_1x_1 + \dots + a_nx_n = b,$$

где коэффициенты $a_1, \dots, a_n$ и b принадлежат кольцу A и среди $a_1, \dots, a_n$ имеются отличные от нуля. Часто для кратности мы будем говорить, что линейное уравнение принадлежит кольца $A[x_1, \dots, x_n]$, подразумевая, что это уравнение можно привести к виду $f = 0$, $f \in A[x_1, \dots, x_n]$.

Определение 25. Конечное множество уравнений из кольца $A[x_1, \dots, x_n]$ будем системой уравнений.

В Sage система уравнений представляется как список уравнений или многочленов. Напр.,

```
sage: var("x,y")
```

```
(x, y)
sage: solve([x+y-1, x-y-2],[x,y])
[
[x == (3/2), y == (-1/2)]
]
sage: solve([x+y==1, x-y==2],[x,y])
[
[x == (3/2), y == (-1/2)]
]
```

Функция `solve(eqs,vars)` пришла в Sage из древних времен, она корректно решает системы линейных уравнений над $\mathbb{Q}$, однако не умеет работать с другими полями.

Если A вложено в некоторое кольцо B, то мы можем говорить о значении многочлена из $A[x_1, \ldots, x_n]$ в любой точке, координаты которой принадлежат B.

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. Напр.,

```
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
```

Аргументом выступает список. Можно подставлять и в элемент кольца непосредственно:

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

```
29/6
```

Вариант со списком не работает. Дело в том, что переменные, на место которых что-то можно подставлять, в кольце перенумерованы, начиная с 0. Поэтому поддерживается вот такой вариант:

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

Таким образом, при подстановке в многочлены вместо списков предлагается использовать словари.

Определение 26. Пусть A вложено в некоторое кольцо B. Точка $(c_1, \ldots, c_n)$, координаты которой принадлежат кольцу B, называется решением системы S линейных уравнений над A с неизвестными $x_1, \ldots x_n$, если каждое из уравнений системы обращается в нуль при подстановке $x_1 = c_1, \ldots, x_n = c_n$. Множество всех решений обозначается как $\mathrm{Sol}(S, B)$.

Решение систем линейных уравнений в $\mathbb{Q}$ входит в школьную программу. Посмотрим, что там предлагают сделать.

Пример 4. Чтобы решить систему

$$\begin{cases} x + y = 1, \\ x - y = 2 \end{cases}$$

из второго уравнения вычитают первое и получают систему «треугольного вида»

$$\begin{cases} x + y = 1, \\ -2y = 1 \end{cases}$$

эквивалентную исходной. Из последнего уравнения находят $y = -1/2$, подставляют это значение в первое уравнение и получают $x - 1/2 = 1$, откуда находят x.

По существу решение осуществляет в два этапа: приведение к треугольному виду и решение треугольной системы. При этом первый этап делается в $\mathbb{Z}$, а второй — в $\mathbb{Q}$. Нам предстоит описать в общем виде, что такое треугольная система и что такое система, эквивалентная исходной.

4.2. Приведение линейной системы к треугольному виду

Определение 27. Система линейных уравнений $T = \{f_1, \ldots, f_r\}$ из кольца $A[x_1, \ldots, x_n]$ называется треугольной, если

$$\mathrm{lm}(f_1) > \mathrm{lm}(f_2) > \cdots > \mathrm{lm}(f_r).$$

Пример 5.
```
sage: var("x1,x2,x3,x4")
(x1, x2, x3, x4)
sage: K=ZZ[x1,x2,x3,x4]
sage: T=[x1+x2+2*x3-2,3*x3+x4]
```

Система T имеет треугольную форму, поскольку:

```
sage: [K(t).lm() for t in T]
[x1, x3]
sage: K(x1)>K(x3)
True
```

Определение 28. Две системы линейных уравнений S_1 и S_2 над кольцом A называются эквивалентными, если для любого кольца B, содержащего A, верно:

$$\mathrm{Sol}(S_1, B) = \mathrm{Sol}(S_2, B).$$

Мы дали это определение таким образом, что эквивалентность двух систем на зависит от B.

Теорема 10. Пусть S — система линейных уравнений над кольцом A. Если к одному из уравнений системы прибавить другое, умноженное на элемент кольца A, то получится система, эквивалентная исходной.

Доказательство. Пусть первое уравнение — это $f = 0$, а второе $g = 0$, а все прочие уравнения образуют систему S'. Тогда исходная система S_1 есть объединение $[f = 0, g = 0]$ и S', а полученная из нее система S_2 есть объединение $[f + ag = 0, g = 0]$, где $a \in A$, и S'.

Если точка c принадлежит $\mathrm{Sol}(S_1, B)$, то

$$f|_{x=c} = 0, \quad g|_{x=c} = 0, \quad h|_{x=c} = 0 \quad \forall h \in S'.$$

Но тогда

$$(f + ag)|_{x=c} = 0, \quad g|_{x=c} = 0, \quad h|_{x=c} = 0 \quad \forall h \in S',$$

то есть $c \in \mathrm{Sol}(S_2, B)$.

Если точка c принадлежит $\mathrm{Sol}(S_2, B)$, то

$$(f + ag)|_{x=c} = 0, \quad g|_{x=c} = 0, \quad h|_{x=c} = 0 \quad \forall h \in S'.$$

Но тогда

$$(f + ag - ag)|_{x=c} = 0, \quad g|_{x=c} = 0, \quad h|_{x=c} = 0,$$

то есть $c \in \mathrm{Sol}(S_1, B)$. Таким образом, вне зависимости от выбора B верно, что $\mathrm{Sol}(S_1, B) = \mathrm{Sol}(S_2, B)$. $\square$

Теорема 11. Пусть S — система линейных уравнений над целостным кольцом A. Если одно из уравнений умножить на элемент кольца A, то получится система, эквивалентная исходной.

Доказательство очевидно, но нужно подчеркнуть, что теорема верна только для целостных колец.

Теорема 12. Всякая линейная система над целостным кольцом или приводится к треугольному виду, или не имеет решения ни в одном из расширений этого кольца.

Мы дадим конструктивное доказательство теоремы 12. Пусть S — заданная система уравнений из $A[x_1, \dots, x_n]$, L, T — пока пустые множества уравнений. Будем преобразовывать систему по теоремам 10 и 11 так, чтобы исходная система была на каждом шаге эквивалентна объединению S, а в конце S оказалось пустым, а T — треугольной системой. L будет вспомогательным множеством.

Один шаг опишем так. Пусть $T+S$ эквивалентно исходной системе и T пусто или

$$\mathrm{lm}(f) < \mathrm{lm}(t) \quad \forall f \in S,\, t \in T.$$

Прежде всего найдем

$$m = \max_{f \in S} \mathrm{lm}(f)$$

и положим

$$L = \{f \in S : \quad \mathrm{lm}(f) = m\}, \quad S = \{f \in S : \quad \mathrm{lm}(f) < m\}$$

Тогда исходной системе эквивалентно система $T + L + S$. Пусть для определенности

$$L = (g_1, \ldots, g_k).$$

Добавим первый элемент g_1 множества L к T, что не меняет треугольной формы этого множества, поскольку

$$m < \mathrm{lm}(t) \quad \forall t \in T.$$

Переберем теперь все оставшиеся g из L. Поскольку

$$g_i = \mathrm{lc}(g_i)m + \ldots$$

разность

$$g_i' = \mathrm{lc}(g_1)g_i - \mathrm{lc}(g_i)g_1$$

не содержит монома m, т.е.

$$\mathrm{lm}(g_i') < m.$$

Если степень g_i' равна -1, то этот многочлен сводится к 0, что дает тривиальное уравнение $0 = 0$, которое мы просто отбросим. Если степень g_i' равна 0, то это дает уравнение вида $1 = 0$, которое не может иметь решения, поскольку A — целостное кольцо. Если же степень равна 1, то получается линейное уравнение. Добавим его к списку S. Сделав это со всеми g из L, мы получим два множества $T \neq \emptyset$ и S, причем $T + S$ будет эквивалентна исходной и

$$\mathrm{lm}(f) < m \leq \mathrm{lm}(t) \quad \forall f \in S,\, t \in T.$$

Делая такие шаги мы будем каждый раз увеличивать T и уменьшать S хотя бы на один элемент. Поэтому за конечное число шагов мы придем к $S = \emptyset$ и тем самым приведем систему к треугольному виду.

Описанный алгоритм приведения произвольной системы к системе треугольного вида часто называют алгоритмом Гаусса. В Sage его можно реализовать в виде функции (см. алгоритм 1). Рассмотрим несколько примеров.

Algorithm 1 Приведение системы линейных уравнений к треугольному виду (алгоритм Гаусса)

```
def triangulation(S):
    T=[]
    while S!=[]:
        m=max([s.lm() for s in S])
        L = [s for s in S if s.lm() == m]
        S = [s for s in S if s.lm() < m]
        g1=L[0]
        T.append(g1)
        for g in L[1:]:
            g=g1.lc()*g-g.lc()*g1
            if g.degree()==0:
                T=[1]
                break
            elif g.degree()==1:
                S.append(g)
    return T
```

Для систем над кольцом $\mathbb{Z}$:

```
sage: var("x,y,z")
(x, y, z)
```

```
sage: K=ZZ[x,y,z]
sage: triangulation([K(x+2*y+z-3),K(x+y),K(x+2*y+1)])
[x + 2*y + z - 3, -y - z + 3, -z + 4]
sage: triangulation([K(x+2*y+z-3),K(x+y),K(x+y+1)])
[1]
sage: triangulation([K(x+2*y+z-3),K(x+y),K(x+y+x+2*y+z-3)])
[x + 2*y + z - 3, -y - z + 3]
```

Системы с параметром можно описать как системы над кольцом $\mathbb{Z}[t]$:

```
sage: var("t")
t
sage: K=ZZ[t][x,y,z]
sage: triangulation([K(x+t*y+z-3),K(x+y),K(x+2*y+t^2)])
[x + t*y + z - 3, (-t + 1)*y - z + 3, z - t^3 + t^2 - 3]
```

4.3. Решение треугольной системы наибольшего ранга

Определение 29. Число уравнений треугольной системы называется ее рангом (rank).

Рассмотрим случай, когда ранг имеет наибольшее из возможных значений, то есть равен числу неизвестных.

Старшие мономы линейных многочленов из треугольной системы $T = (f_1, \ldots, f_r)$ должны быть все различны, а всего линейных мономов имеется n: $x_1 > x_2 > \cdots > x_n$, то при $r = n$ мы имеем

$$\mathrm{lm}(f_i) = x_i.$$

Поэтому уравнения системы устроены следующим образом:

$$\begin{cases} a_1x_1 + \cdots = 0 \\ a_2x_2 + \cdots = 0 \\ \ldots \\ a_nx_n + b_n = 0 \end{cases}$$

В поле частных кольца A последнее уравнение однозначно определяет x_n. После подстановки этого значения вместо x_n предпоследнее уравнение определяет x_{n-1} и т.д.

Теорема 13. Пусть A — целостное кольцо. Треугольная система T уравнений из $A[x_1, \ldots, x_n]$ ранга n имеет и притом единственное решение в поле частных кольца A.

Algorithm 2 Решение треугольной системы наибольшего ранга

```
def tsolve(T):
    n=len(T)
    [a,b]=T[-1].coefficients()
    S=[-b/a]
    for i in range(n-1):
        T=[t.subs({n-1-i:-b/a}) for t in T[:len(T)-1]]
        [a,b]=T[-1].coefficients()
        S.append(-b/a)
    S.reverse()
    return S
```

Описанный примем можно реализовать в виде функции в Sage (см. алгоритм 2). Напр.,

```
sage: K=QQ[x,y,z]
sage: T=triangulation([K(x+2*y+z-3),K(x+y),K(8*x+2*y
   +1)])
sage: tsolve(T)
[-1/6, 1/6, 17/6]
```

4.4. Решение системы линейных уравнений

Задача 1. Дана система линейных уравнений над целостным кольцом. Требуется найти решение это системы в поле частных исходного кольца.

Задача решается в два этапа:

1) приведение системы к треугольному виду,

2) решение треугольной системы.

Обычно на первом этапе получается система наибольшего ранга.

Определение 30. Под рангом произвольной системы линейных уравнений понимают ранг эквивалентной ей треугольной системы.

Замечание. Можно доказать, что ранг системы не зависит от способа построения треугольной системы.

Тут могут представиться три случая.

1. Если ранг совпадает с числом неизвестных, то множество решений состоит из одной точки.

Чтобы генерировать нетривиальные тестовые примеры в Sage, удобно использовать метод `random_element`, который возвращает случайный элемент того множества, к которому он применен.

Создадим список из 10 неизвестных:

```
sage: x=var(['x'+str(n) for n in range(10)])
sage: x
(x0, x1, x2, x3, x4, x5, x6, x7, x8, x9)
sage: K=QQ[x]
sage: K
Multivariate Polynomial Ring in x0, x1, x2, x3, x4,
   x5, x6, x7, x8, x9 over Rational Field
```

Создадим список из 10 линейных уравнений со случайными целыми коэффициентами:

```
sage: S=[K(sum([ZZ.random_element()*t for t in x]) +
    ZZ.random_element()) for tt  in x]
sage: S
[x0 - 53*x1 + 4*x2 - 8*x3 + x4 - x5 - x6 + 32*x7 +
   x8 + 3, x0 - 4*x1 + x2 - 205*x3 + 4*x4 - 8*x5 + x6
    - x7 - x9 - 14, 3*x0 + 2*x1 - x2 - x4 + 3*x5 + x7
    + x9 + 5, -x1 + 2*x2 + x3 - 20*x4 - 3*x5 - x6 +
   x7 - 7*x8, -x0 + 3*x1 - x2 + 4*x3 + 5*x4 - x5 + 2*
   x6 + x8 + 2*x9 + 2, x0 + x1 + x2 - 3*x3 + 2*x5 -
   x6 + x7 + 2*x9 + 7, x0 + x1 + x2 + x4 + 4*x5 + 2*
   x6 - x7 - 4*x8 - 16*x9 + 1, -6*x2 - 24*x3 + 4*x4 +
    5*x5 + x6 - 2*x7 + x8 - 3*x9 - 2, 2*x0 + x1 + 11*
   x2 + 5*x3 - x4 - x5 + x8 + 1, -2*x0 + 26*x1 - 5*x2
    + x4 - x6 - 4*x7 + x9 - 1]
```

Триангуляция дает:

```
sage: T=triangulation(S)
sage: T
[x0 - 53*x1 + 4*x2 - 8*x3 + x4 - x5 - x6 + 32*x7 +
   x8 + 3, -x1 + 2*x2 + x3 - 20*x4 - 3*x5 - x6 + x7 -
    7*x8, -6*x2 - 24*x3 + 4*x4 + 5*x5 + x6 - 2*x7 +
   x8 - 3*x9 - 2, -3168*x3 - 5482*x4 - 449*x5 - 187*
   x6 - 94*x7 - 1969*x8 - 291*x9 - 292, 22796652*x4 +
    1340862*x5 + 845130*x6 + 110532*x7 + 8083614*x8 +
    1082682*x9 + 192504, 669007506816*x5 -
   713678283648*x6 - 1153122676992*x7 + 262882578816*
   x8 - 1110395392128*x9 - 1507749686784,
   -486141299713356605227008*x6 -
   1362116722976745538682880*x7 +
   313203720823445418835968*x8 -
```

```
1440470914658671710633984*x9 -
3164339138295413245280256,
-1792365605107598403460734290216420346559815745536*
x7 -
271072219789425343489790894283319593447179943936*
x8 -
4176510962547038012830875454940516972182791782400*
x9 -
4815440674691928554535799380492819123745931132928,

-16754014314772802970101639436845764271504658482323071631
x8 -
488184157561416584788475365113848761614871187232884982390
x9 +
341287461937845007953747182965393655307694974704664724385

-10440008248011674189200366655330344623111124636086122569
x9 -
142576940938880473383524565229237027351032809453466796133
```

Обратите внимание на гигантские коэффициенты последнего уравнения. тем не менее, эта система имеет единственное решение:

```
sage: tsolve(T)
[-5906968819/10235488888, -103146779/10235488888,
  -746740541/1279436111, -430620097/10235488888,
  -14088271093/10235488888, -1580484558/1279436111,
  788661598/1279436111, -1402424039/10235488888,
  42815716065/10235488888, -13978386415/10235488888]
```

2. Ранг равен 0, т.е. триангуляция приводит к уравнению $1 = 0$. В этом

случае система не имеет решений.

3. Если триангуляция приводит к системе $T = (t_1, \dots, t_r)$, ранг которой меньше n, то список

$$(\mathrm{lm}(t_1), \dots, \mathrm{lm}(t_r)) \subset (x_1, \dots, x_n)$$

Добавим к T уравнения

$$x_i = b_i, \quad x_i \notin (\mathrm{lm}(t1), \dots, \mathrm{lm}(t_r))$$

где b_i — любые элементы поля частного. Тогда получится треугольная система наибольшего ранга, которая имеет единственное решение. Добавление уравнений уменьшает множество решений, поэтому это решение будет и решением исходной. Следовательно, таким путем можно найти различные решения исходной системы.

Если поле частных — бесконечное, то система имеет бесконечно много значений. Мы выделим одно единственное решение, если придадим $n - r$ неизвестным, не входящим в список $(\mathrm{lm}(t_1), \dots, \mathrm{lm}(t_r))$, произвольные значения.

Пример 6. Рассмотрим систему:

```
sage: K=QQ[x0,x1,x2,x3]
sage: S=[K(x0+2*x1-3*x2 + x3-1), K(3*x0-2*x1-3*x2 +
    3*x3+1),K(4*x0 - 6*x2 + 4*x3),K(-5*x0 + 6*x1 + 3*
    x2 - 5*x3 - 3)]
sage: S
[x0 + 2*x1 - 3*x2 + x3 - 1, 3*x0 - 2*x1 - 3*x2 + 3*
    x3 + 1, 4*x0 - 6*x2 + 4*x3, -5*x0 + 6*x1 + 3*x2 -
    5*x3 - 3]
```

Триангуляция дает только два уравнения:

```
sage: T=triangulation(S)
sage: T
```

```
[x0 + 2*x1 - 3*x2 + x3 - 1, -8*x1 + 6*x2 + 4]
sage: [K(t).lm() for t in T]
[x0, x1]
```

Старшими мономами будут

```
sage: [K(t).lm() for t in T]
[x0, x1]
```

Поэтому x_3 и x_4 мы можем брать любыми. Напр.,

```
sage: tsolve(T+[K(x2-1),K(x3-2)])
[-1/2, 5/4, 1, 2]
```

4.5. Задания

Теоретические задания.

1) Дайте определения линейного уравнения, системы линейных уравнений и ее решения.
2) Дайте определение треугольной системы линейных уравнений.
3) Опишите алгоритм приведения системы к треугольному виду. Какие теоремы при этом используются?
4) Как устроено решение треугольной системы?

Практические задания.

1) Дана система уравнений

$$x - 5y + z = 3, \quad 3x - 2y + 2z = 1, \quad 8y + 2z = -3$$

   из $\mathbb{Z}[x, y, z]$.

   a) Приведите ее к треугольному виду, приняв $x > y > z$.

б) Приведите ее к треугольному виду, приняв $x < y < z$.

2) Найдите решение системы

$$x - 5y + z = 3, \quad 3x - 2y + 2z = 1, \quad 8y + 2z = -3$$

a.) в кольце $\mathbb{Z}$, b.) в поле $\mathbb{Q}$, c.) в кольце $\mathbb{Q}[t]$.

3) Определите ранг системы

а) $x - 5y + z = 3, \quad 3x - 2y + 2z = 1, \quad 8y + 2z = -3$

б) $x - 5y + z = 3, \quad 3x - 2y + 2z = 1, \quad -7x - 4y - 4z = 3$

в) $x - 5y + z = 3, \quad 3x - 2y + 2z = 1, \quad -7x - 4y - 4z = 4$

из $\mathbb{Z}[x, y, z]$. Укажите, в каком случае система имеет бесконечно много решений в $\mathbb{Q}$.

4) Дана система уравнений

$$tx - 5y + z = 3, \quad 3x - ty + 2z = 1, \quad 8y + tz = -3$$

из $\mathbb{Z}[t][x, y, z]$. Приведите ее к треугольному виду.

5) Создайте и решите систему линейных 20 уравнений с 20 неизвестными и случайными коэффициентами.