Идеалы и факторкольца

М.Д. Малых, РУДН

6 октября 2022 г.

Содержание

1. Идеалы

Исторически арифметика и алгебра развивались параллельно, однако их методы всегда были подозрительно схожи. Феликс Клейн в конце XIX выдвинул амбициозную программу создания единой теории, в которой алгебраические числа и алгебраические функции рассматривались с единой точки зрения. Ключевой идеей, объединивший арифметику и алгебру, стало понятие идеала.

1.1. Определения

Определение 1. Подмножество J кольца A называется идеалом (ideal), если для любого $a \in A$ и любых $b, c \in J$ верно следующее:

1) для любого $a \in A$ и любого $b \in J$ произведение ab принадлежит J;

2) для любых $b, c \in J$ сумма $b + c$ принадлежит J.

Теорема 1. Если 1 принадлежит идеалу J кольца A, то $J = A$.

Теорема 2. Пусть S — конечное множество элементов кольца A, тогда множество элементов вида

$$\sum_{s \in S} a_s s$$

образует идеал.

Определение 2. Пусть S — конечное множество элементов кольца A, тогда множество элементов вида

$$\sum_{s \in S} a_s s$$

называют идеал, порожденным множеством S.

В Sage используется единое обозначение для идеалов. Они всегда задаются путем указания множества S. Это множество задается как список `[s1, ..., sr]`, а идеал кольца `A`, порожденный этим списком, как `A*[s1,...,sr]`.

Определение 3. Идеал, порожденным множеством S, состоящим из одного элемента, называют главным (principal).

Определение 4. Кольцо, в котором все идеалы — главные, называют кольцом главных идеалов.

В центре внимания компьютерной алгебры лежит следующая задача.

Задача 1. Дано кольцо A, идеал этого кольца J и элемент f этого кольца. Требуется выяснить, принадлежит ли f идеалу J.

Для некоторых колец она решается конструктивно.

1.2. Идеалы кольца $\mathbb{Z}$

Пусть q — целое число, тогда множество всех чисел вида aq, где $a \in \mathbb{ZZ}$, является главным идеалом, который обозначают как (q) или $q\mathbb{Z}$. Иными словами, множество всех целых чисел, которые делятся на число q, является идеалом $q\mathbb{Z}$. Напр., множество четных чисел является главным идеалом.

```
sage: ZZ*[2]
Principal ideal (2) of Integer Ring
sage: 2*ZZ
Principal ideal (2) of Integer Ring
```

Идеалы $(-q)$ и (q) совпадают, поэтому по умолчанию считают q натуральным числом:

```
sage: ZZ*[-2]
Principal ideal (2) of Integer Ring
```

Определение 5. Пусть два целых числа a и q связаны соотношением

$$a = nq + r, \quad 0 \leq r < q,$$

тогда n называют частным (quotient) от деления a на q, а r — остатком (reminder).

Отыскание частного и остатка по заданным a и q является тривиальной задачей. Сначала постепенно увеличивая n от нуля мы находим такое значение n, что

$$(n+1)q > a > nq.$$

Затем, вычисляем r как $a - nq$. Отыскать частное и остаток в Sage можно способом, описанным в алгоритме 1:

```
sage: quo_rem_ZZ(28,5)
(5, 3)
```

Algorithm 1 Алгоритм деления в $\mathbb{Z}$

```
def quo_rem_ZZ(a,q):
    n=0
    b=abs(a)
    while b>(n+1)*q:
        n=n+1
    if a>0:
        ans=(n,a-n*q)
    else:
        ans=(-(n+1),a+(n+1)*q)
    return ans
```

Но лучше и быстрее это сделать при помощи встроенной функции функцииquo_rem, которая, как и наша, возвращает список, первый элемент которого частное от деления, второй — остаток:

```
sage: 28.quo_rem(5)
(5, 3)
```

Алгоритм деления позволяет решить задачу 1 для главных идеалов.

Теорема 3. Целое число a принадлежит главному идеалу $q\mathbb{Z}$, если a делится на q без остатка.

В нашем примере $28 \notin 5\mathbb{Z}$. Решение задачи 1 для кольца целых чисел встроено в Sage:

```
sage: 18 in 5*ZZ
False
```

Более того, алгоритм деления позволяет доказать, что $\mathbb{Z}$ — кольцо главных идеалов.

Теорема 4. Всякий идеал кольца $\mathbb{Z}$ является главным.

Доказательство. Пусть J — идеал кольца $\mathbb{Z}$, и пусть q — наименьшее натуральное число, принадлежащее J. Любое число $a \in J$ можно поделить на q:

$$a = nq + r, \quad 0 \leq r < q.$$

Но тогда $r = a - nq \in J$ или 0, или натуральное число, которое строго меньше q. Второе невозможно, поэтому всякий элемент идеала J делится на q, то есть $J = q\mathbb{Z}$. □

1.3. Идеалы кольца $\mathbb{Q}[x]$

В полной аналогии с кольцом $\mathbb{Z}$ главный идеал (q) кольца $\mathbb{Q}[x]$ образован всеми многочленами, которые делятся на q. В Sage идеал (x^2+3) задается так:

```
sage: var("x")
x
sage: QQ[x]*[x^2+3]
Principal ideal (x^2 + 3) of Univariate Polynomial Ring in x over Rational Field
```

В кольце $\mathbb{Q}[x]$ можно ввести деление, поэтому оно очень похоже на $\mathbb{Z}$.

Определение 6. Пусть два многочлена f и q связаны соотношением

$$f = nq + r, \quad n, r \in \mathbb{Q}[x], \quad \mathrm{degree}(r) < \mathrm{degree}(q),$$

тогда n называют частным от деления a на q, а r — остатком.

В кольце $\mathbb{Q}[x]$ невозможно перебрать все многочлены, степень которых меньше степени f. Поэтому алгоритм деления устроен сложнее. Итак, пусть нам заданы f и q. Если $\mathrm{degree}(f) < \mathrm{degree}(q)$, то

$$n = 0, \quad r = f.$$

В противном случае, дробь

$$n_1 = \frac{\mathrm{lt}(f)}{\mathrm{lt}(q)}$$

является одночленом нашего кольца, а степень многочлена

$$f_1 = f - n_1 q$$

строго меньше степени f. Если $\mathrm{degree}(f_1) < \mathrm{degree}(q)$, то

$$n = n_1, \quad r = f_1.$$

В противном случае, мы образуем

$$n_2 = \frac{\mathrm{lt}(f_1)}{\mathrm{lt}(q)}$$

и перейдем к рассмотрению многочлена

$$f_2 = f_1 - n_2 q,$$

степень которого строго меньше f_1. Действуя так далее, мы придем к многочлену f_i, степень которого будет меньше степени q. Собирая все вместе, имеем

$$f = n_1 q + f_1, \quad f_1 = n_2 q + f_2, \ldots, f_{i-1} = n_i q + f_i.$$

Отсюда

$$f = n_1 q + f_1 = (n_1 + n_2) q + f_2 = \cdots = (n_1 + \cdots + n_i) q + f_i.$$

Таким образом, $n_1 + \cdots + n_i$ будет частным от деления, а f_i остатком.

Algorithm 2 Алгоритм деления в $\mathbb{Q}[x]$

```
def quo_rem_poly(f,q):
    K=f.parent()
    n=0
    while f.degree()>=q.degree():
        ni=K(f.lt()/q.lt())
        n=n+ni
        f=f-ni*q
    return (n,f)
```

Описанное можно представить в виде алгоритма 2 деления в полиномиальном кольце.

```
sage: K=QQ[x]
sage: quo_rem_poly(K(x^5+3*x-1),K(x-1))
(x^4 + x^3 + x^2 + x + 4, 3)
sage: K(x^5+3*x-1)==K((x^4 + x^3 + x^2 + x + 4)*(x-1)+3)
True
```

Конечно, нам не важно, что коэффициенты многочленов берутся из поля $\mathbb{Q}$, но важно, что они берутся из поля, поскольку при нахождении $n_1 \dots$ мы делим коэффициенты.

В Sage для отыскания частного и остатка рекомендуется использовать уже известную нам функция `quo_rem`:

```
sage: QQ[x](x^2-2).quo_rem(QQ[x](x-1))
(x + 1, -1)
```

Алгоритм деления позволяет решить задачу 1 для главных идеалов и в полиномиальном кольце.

Теорема 5. Многочлен f принадлежит главному идеалу (q), если f делится на q без остатка.

Напр., $x^2 - 2 \notin (x-1)$. Решение задачи 1 для идеалов кольца $\mathbb{Q}[x]$ реализовано в Sage:

```
sage: x^5-2 in QQ[x]*[x^2+3]
True
```

Теорема 6. Всякий идеал кольца $\mathbb{Q}[x]$ является главным.

Доказательство. Пусть J — идеал кольца $\mathbb{Q}[x]$, и пусть q — многочлен наименьшей степени, принадлежащее J. Любой многочлен $a \in J$ можно поделить на q:

$$a = nq + r, \quad 0 \leq \mathrm{degree}(r) < \mathrm{degree}(q).$$

Но тогда $r = a - nq \in J$ или 0, или многочлен, степень которого строго меньше степени многочлена q. Второе невозможно, поэтому всякий элемент идеала J делится на q, то есть $J = (q)$. $\square$

Кольца $\mathbb{Z}$ и $\mathbb{Q}[x]$ — очень похожи, поскольку оба являются кольцами главных идеалов. В Sage идеалы кольца $\mathbb{Q}[x]$ всегда переводятся в главные:

```
sage: QQ[x]*[x-1,x^2-1]
Principal ideal (x - 1) of Univariate Polynomial
   Ring in x over Rational Field
```

1.4. Идеалы кольца $\mathbb{Q}[x, y]$

Пусть $x+y$ и x^2-y — два многочлена кольца $\mathbb{Q}[x, y]$, тогда множество всех многочленов вида

$$f(x+y) + g(x^2-y), \quad f, g \in \mathbb{Q}[x, y]$$

является идеалом кольца $\mathbb{Q}[x, y]$, который обозначается как $(x+y, x^2-y)$. В Sage его можно задать так:

```
sage: var("x,y")
(x, y)
sage: QQ[x,y]*[x+y,x^2-y]
Ideal (x + y, x^2 - y) of Multivariate Polynomial
   Ring in x, y over Rational Field
```

Поскольку на множители многочлены $x+y$ и x^2-y не раскладываются, этот идеал не может оказаться главным.

Кольцо $\mathbb{Q}[x_1, \ldots, x_n]$ при $n > 1$ не является кольцом главных идеалов и решение в нем задачи 1 представляет собой фундаментальную проблему, решенную лишь в середине XX века, благодаря сочетанию идеи деления и идеи метода Гаусса. Мы вернемся к этому вопросу позже.

2. Факторкольца

2.1. Определения

Пусть J — идеал кольца A. Введем на A отношение эквивалентности, приняв, что

$$a \sim b$$

означает, что $a - b \in J$. При этом выполняются аксиомы:

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 $a \sim c$.

Введем на фактормножестве $A/\sim$ арифметические действия:

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

Это определение корректно в том смысле, что сумма и произведение $[a]$ и $[b]$ зависит от классов, но не от выбора представителей этих классов. В самом деле, пусть

$$a' \in [a], \quad b' \in [b]$$

то есть $[a'] = [a]$ и $[b'] = [b]$, тогда

$$a' + b' - a - b = (a' - a) + (b' - b) \in J$$

и поэтому $[a + b] = [a' + b']$, и

$$a'b' - ab = a'b' - ab' + ab' - ab = (a' - a)b' + a(b - b') \in J$$

и поэтому $[ab] = [a'b']$.

Фактормножество с так введенными арифметическими действиями является кольцом.

Определение 7. Пусть J — идеал кольца A. Приняв, что элементы A эквивалентны, если их разность принадлежит идеалу J, мы получим фактормножество $A/\sim$, которое мы превратим в кольцо, приняв

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

Это фактормножество с так введенными арифметическими действиями называют факторкольцом (quotient ring) и пишут A/J.

В Sage имеется общая конструкция для задания факторкольца кольца A по идеалу J: `A.quotient_ring(J)` или, короче, `A.quotient(J)`.

2.2. Факторкольца кольца $\mathbb{Z}$

Всякий идеал кольца $\mathbb{Z}$ является главным и всякое натуральное число порождает главный идеал кольца $\mathbb{Z}$.

Определение 8. Факторкольцо $\mathbb{Z}/q\mathbb{Z}$ называют кольцом целых чисел по модулю q (ring of integers modulo q).

В Sage кольцо $\mathbb{Z}/5\mathbb{Z}$ задается любым из следующих способов:

```
sage: ZZ.quotient_ring(ZZ*[5])
Ring of integers modulo 5
sage: ZZ.quotient(ZZ*[5])
Ring of integers modulo 5
sage: ZZ.quotient(5*ZZ)
Ring of integers modulo 5
```

Элементом кольца $\mathbb{Z}/q\mathbb{Z}$ является класс эквивалентности

$$[a] = a + q\mathbb{Z}.$$

В Sage любое целое число a можно рассматривать как элемент $[a]$ кольца $\mathbb{Z}/5\mathbb{Z}$:

```
sage: A=ZZ.quotient(5*ZZ)
```

```
sage: 8 in A
True
sage: A(8)
3
```

Как видно, в качестве представителя класса $[a]$ берут наименьшее положительное число, принадлежащее классу. Напр., для класса $6 + 5\mathbb{Z}$ таковым будет 1. При этом, напр., для факторкольца $\mathbb{Z}/5\mathbb{Z}$ верно

$$[1] + [4] = [1 + 4] = [0]$$

и

$$[2] \cdot [4] = [8] = [3]$$

В нотации Sage эти равенства выглядят так:

```
sage: A(1)+A(4)
0
sage: A(2)*A(4)
3
```

Традиционно квадратные скобки опускают и эти формулы записывают короче:

$$1 + 4 = 0 \mod 5$$

и

$$2 \cdot 4 = 3 \mod 5$$

Запись $\mod 5$ можно понимать в том смысле, что целые числа рассматриваются как указатели для классов эквивалентности факторкольца $\mathbb{Z}/5\mathbb{Z}$, содержащих эти числа. Допустим и более простой взгляд, $1 + 4 = 5$ отличается от 0 на элемент идеала $5\mathbb{Z}$, то есть равен нулю по модулю 5. В Sage есть аналогичная короткая запись:

```
sage: 1+4 % 5
5
```

```
sage: 2*4 % 5
3
```

Эта новая «арифметика» была создана Гауссом за долго до появления теории идеалов и получила названия модулярной арифметики. Этим путем получается множество новых колец, к изучению которых мы перейдем в следующем разделе.

2.3. Факторкольца кольца $\mathbb{Q}[x]$

Всякий идеал кольца $\mathbb{Q}[x]$ является главным и всякий многочлен q порождает главный идеал (q) кольца $\mathbb{Q}[x]$. В Sage факторкольцо кольцо $\mathbb{Q}[x]/(q)$ задается любым из следующих способов:

```
sage: QQ[x].quotient(x^2+1)
Univariate Quotient Polynomial Ring in xbar over
   Rational Field with modulus x^2 + 1
```

Элементом этого кольца является класс эквивалентности

$$[f] = f + q\mathbb{Q}[x],$$

который в Sage задается обычным путем. Напр., элемент $[x^3]$ факторкольца $\mathbb{Q}[x]/(x^2+1)$ задается так

```
sage: A=QQ[x].quotient(x^2+1)
sage: A(x^3)
-xbar
```

Как видно, в качестве представителя класса $[a]$ берут многочлен наименьшей степени, принадлежащий этому классу и при этом по умолчанию вместо x пишут `xbar`. Если хочется использовать другую букву, нужно указать ее при задании факторкольца следующим образом:

```
sage: A.<i>=QQ[x].quotient(x^2+1)
sage: A(x^3)
```

```
-i
sage: i^2+1
0
```

Это дает нам еще один способ строить новые кольца, в том числе ввести комплексные числа.

3. Задания

Теоретические задания.

1) Дайте определение идеала, главного идеала.
2) Докажите, что кольцо $\mathbb{Z}$ — кольцо главных идеалов.
3) Докажите, что кольцо $\mathbb{Q}[x]$ — кольцо главных идеалов.
4) Дайте определение факторкольца.
5) Докажите, что арифметические действия, введенные в определении факторкольца, удовлетворяют аксиомам кольца.

Практические задания.

1) Выясните, принадлежит ли 5 идеалу $4\mathbb{Z}$.
2) Выясните, принадлежит ли x^3 идеалу $(x^3 + 1)$.
3) Задайте в Sage факторкольца $\mathbb{Z}/8\mathbb{Z}$ и $\mathbb{Q}[x]/(x^3 + 1)$.