Факторкольца кольца многочленов $k[x]$ и комплексные числа

М.Д. Малых, РУДН

20 октября 2022 г.

Содержание

1. Кольцо многочленов $k[x]$

Пусть k — произвольное поле. Множество многочленов, коэффициенты которых принадлежат этому полю, обозначают как $k[x]$. В сравнении с рассмотренным ранее случаем $\mathbb{Q}[x]$ здесь нужно сделать лишь дну существенную оговорку.

В школьном курсе два многочлена p и q из $\mathbb{Q}[x]$ считаются равными, если они принимают одни и те же значения:

$$p(x) = q(x) \quad \forall x \in \mathbb{Q}.$$

Отсюда выводят, что коэффициенты двух равных многочленов совпадают. При работе с конечными полями такое определение равенства использовать нельзя. В самом деле, в GF(2) всего две точки и два значения. Поэтому все многочлены можно разбить на 4 класса. Будем далее будем сравнивать многочлены по коэффициентам: многочлены называются равными, если совпадают коэффициенты их нормальной формы.

2. Факторкольца кольца многочленов

Всякий идеал кольца $\mathbb{Q}[x]$ является главным и всякий многочлен q порождает главный идеал (q) кольца $\mathbb{Q}[x]$. Два многочлена относят к одному классу факторкольца $\mathbb{Q}[x]/(q)$, если их разность делится на q. Поэтому всякий элемент $[f]$ факторкольца можно описать как $[r]$, где r — остаток от деления f на q. Как и в случае кольца целых чисел, обычно в качестве элементов фактокольца $k[x]/(q)$ рассматривают сами остатки, то есть всевозможные многочлены, степень которых меньше степени q.

3. Факторкольца вида $k[x]/(x-a)$

Пусть a — элемент поля k, тогда $x - a$ — многочлен первой степени кольца $k[x]$, а элементами $k[x]/(x-a)$ будет всевозможные многочлены нулевой степени, то есть

$$\daleth[x]/(x-a) = k.$$

При делении многочлена f на $x - a$ мы представляем его в виде

$$f = g \cdot (x-a) + r, \quad r \in k.$$

Подставляя сюда $x = a$, мы видим, что $r = f(a)$.

В элементарной математике многочлен рассматривают как функцию x. Теперь мы можем описать эту функцию на языке идеалов. Всякий элемент $f \in k[x]$ задает функцию, которая ставит в соответствие идеалу J элемент $[f]$ факторкольца $k[x]/J$. В «точке» $J = (x - a)$ эта функция равна $f(a)$, как об этом и говорят в элементарной математике. Это позволяет сократить пропасть между арифметикой и алгеброй. Целое число n тоже задает функцию, которая ставит в соответствие идеалу (q) элемент $[n]$ факторкольца $\mathbb{Z}/(q)$.

4. Факторкольца вида $k[x]/(q)$

Обратимся теперь к случаю, когда степень q больше 1. Как мы знаем,

$$\mathrm{degree}(fg) = \mathrm{degree}(f)\,\mathrm{degree}(g),$$

поэтому $\mathrm{degree}(fg) \geq \mathrm{degree}(f)$.

Определение 1. Многочлен кольца $k[x]$ степени 1 и выше называют неприводимым или простым, если его нельзя представить в виде произведения двух многочленов кольца $k[x]$, степени которых строго больше 0, но меньше степени исходного многочлена.

Ключевым моментом в этом определении является фиксация кольца A. Один и тот же многочлен может быть простым как элемент одного кольца, и не быть таковым в другом.

Пример 1. Число $\sqrt{2}$ не является рациональным, поэтому многочлен x^2-2 как элемент кольца $\mathbb{Q}[x]$ является простым:

```
sage: var("x")
x
sage: QQ[x](x^2-2).is_prime()
True
```

В самом деле, если бы $x^2 - 2$ не был простым, то его можно было бы представить как произведение двух линейных многочленов

$$x^2 - 2 = (ax + b)(cx + d), \quad a, b, c, d \in \mathbb{Q}.$$

Но тогда уравнение $x^2 = 2$ имеет два рациональных корня, один из которых совпадает с $\sqrt{2}$, что невозможно. В то же время, $x^2 - 2$ раскладывается на множители как элемент $\mathbb{R}[x]$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

в чем можно убедиться и так:

```
sage: RR[x](x^2-2).is_prime()
False
```

Теорема 1. Если q — не является простым многочленом кольца $k[x]$, то факторкольцо $k[x]/(q)$ имеет делители нуля.

Доказательство. Поскольку q не является простым, то его можно представить в виде произведения двух многочленов f и g, степени которых заключены между 0 и степенью q. Но тогда $f + (q)$ и $g + (q)$ отличаются от $0 + (q)$, то есть нуля факторкольца, и в то же время

$$(f + (q)) \cdot (g + (q)) = fg + (q) = (q)$$

то есть $f + (q)$ и $g + (q)$ являются делителями нуля в факторкольце. $\square$

Теорема 2. Если p — простой многочлен кольца $k[x]$, то факторкольцо $k[x]/(p)$ является полем.

Доказательство. Пусть $f + (p)$ — произвольный элемент факторкольца, отличный от нуля. Нам нужно предъявить такой элемент этого кольца, скажем, $g + (p)$, что

$$(f + (p)) \cdot (g + (p)) = 1 + (p)$$

или

$$fg + (p) = 1 + (p).$$

Поскольку всякий идеал кольца $k[x]$ является главным, идеал (f, p) можно записать как идеал (q). Запись $f, p \in (q)$ означает, что f и p делятся q. Поскольку p — простой, или $q = 1$, или $q = p$. Во втором случае, f делится на p и $f + (p)$ — нуль факторкольца, что невозможно. Следовательно, $q = 1$ и поэтому $(f, p) = k[x]$. В частности $1 \in (f, p)$, т.е. существуют такие многочлены u и v, что $1 = uf + vp$. Но тогда при $g = u$ мы имеем

$$fg + (p) = fu + (p) = 1 - vp + (p) = 1 + (p),$$

то есть $u + (p)$ — элемент, обратный к $f + (p)$. $\square$

Напр.,

```
sage: QQ[x].quo(x^2+1).is_field()
True
sage: QQ[x].quo(x^2-1).is_field()
False
sage: QQ[x].quo(x^2-2).is_field()
True
```

5. Расширение поля рациональных чисел, содержащее $\sqrt{2}$

Факторкольцо $\mathbb{Q}[x]/(x^2 - 2)$ является полем. Элементами этого пуля будут множества многочленов

$$[f] = f + (x^2 - 2)$$

и, как и в случае целых чисел, обычно в качестве представителя класса $[f]$ берут остаток от деления f на $x^2 - 2$, то есть многочлен, степень которого строго меньше 2. Но тогда любой элемент поля можно записать как

$$[ax + b], \quad a, b \in \mathbb{Q}$$

В силу определения арифметических действий

$$[ax+b]=[a]\cdot[x]+[b].$$

Определение 2. Два кольца A и B называются изоморфными, если между их элементами имеется взаимно однозначное соответствие:

$$f:A\to B,\quad g:B\to A$$

которое согласовано с действиями:

$$f(a+b)=f(a)+f(b),\quad f(ab)=f(a)f(b)\forall a,b\in A$$

и

$$g(a+b)=g(a)+g(b),\quad g(ab)=g(a)g(b)\forall a,b\in B$$

Изоморфные кольца рассматриваются в алгебре как неразличимые.

Подмножество Q факторкольца, образованное всевозможными элементами вида $[b]$, изоморфно полю рациональных чисел. При этом мы сопоставляем числу b класс $[b]=b+(x^2-2)$. Сумма и произведение чисел a и b не зависит от того, рассматриваются ли эти числа как элементы $\mathbb{Q}$ и как элементы факторкольца.

Обычно квадратные скобки опускают, то есть вместо $[a][x]+[b]$ пишут $a[x]+b$. В Sage элемент $[x]$ факторкольца обозначают как `xbar`:

```
sage: QQ[x].quo(x^2-2)
Univariate Quotient Polynomial Ring in xbar over
   Rational Field with modulus x^2 - 2
sage: QQ[x].quo(x^2-2)(2*x+4)
2*xbar + 4
sage: QQ[x].quo(x^2-2)(2*x^3+4)
4*xbar + 4
```

При желании для $[x]$ можно ввести свое обозначение, напр, обозначить его как r:

```
sage: K.<r>=QQ[x].quo(x^2-2)
sage: K(x^3+1)
2*r + 1
```

Нетрудно заметить, что

$$[x]^2 = [x^2] = [x^2 - 2 + 2] = [2] = 2,$$

то есть в поле $\mathbb{Q}[x]/(x^2 - 2)$ уравнение

$$x^2 = 2$$

имеет решение.

С другой стороны, рассмотрим множество A всех чисел вида

$$a\sqrt{2} + b, \quad a, b \in \mathbb{Q},$$

напр., как подмножество в поле $\mathbb{R}$. Арифметические действия не выводят за границы A

$$a\sqrt{2} + b + a'\sqrt{2} + b' = (a + a')\sqrt{2} + b' + b$$

и

$$(a\sqrt{2} + b)(a'\sqrt{2} + b') = (ab' + a'b)\sqrt{2} + 2aa' + b'b$$

и выполнены все аксиомы кольца, поэтому A — кольцо. Обратным к $a\sqrt{2}+b$ будет

$$\frac{1}{a\sqrt{2} + b} = \frac{-a\sqrt{2} + b}{(a\sqrt{2} + b)(-a\sqrt{2} + b)} = \frac{-a\sqrt{2} + b}{b^2 - 2a^2},$$

причем знаменатель не равен нулю, поскольку $a, b \in \mathbb{Q}$, а $\sqrt{2}$ — не рациональное число. Поэтому множество A — поле.

Теорема 3. Факторкольцо $\mathbb{Q}[x]/(x^2 - 2)$ изоморфно множеству всех чисел вида

$$a\sqrt{2} + b, \quad a, b \in \mathbb{Q}.$$

Эта теорема позволяет рассматривать факторкольцо $\mathbb{Q}[x]/(x^2-2)$ как подполе поля $\mathbb{R}$, содержащее поле $\mathbb{Q}$ и оба корня уравнения $x^2=2$:

$$\mathbb{Q} \subset \mathbb{Q}[x]/(x^2-2) \subset \mathbb{R}.$$

Долгое время вопросы о приближенном вычислении $\sqrt{2}$ и символьных манипуляциях с $\sqrt{2}$ рассматривались вместе, однако они относятся к разным областям математики. В алгебре занимаются символьными манипуляциями с корнями уравнения $x^2=2$, для которых не нужно знать значение $\sqrt{2} \simeq 1.4\ldots$ в виде десятичной дроби.

6. Гауссовы рациональные числа

Определение 3. Элементы поля $\mathbb{Q}[x]/(x^2+1)$ будем называть гауссовыми рациональными числами.

Элементами этого поля будут множества многочленов

$$[f] = f + (x^2+1)$$

и, как и в случае целых чисел, обычно в качестве представителя класса $[f]$ берут остаток от деления f на x^2+1, то есть многочлен, степень которого строго меньше 2. Но тогда любой элемент поля можно записать как

$$[ax+b], \quad a, b \in \mathbb{Q}$$

В силу определения арифметических действий

$$[ax+b] = [a]\cdot[x] + [b].$$

Множество всех элементов вида $[b]$ изоморфно полю $\mathbb{Q}$, поэтому поле гауссовых рациональных чисел является расширением поля рациональных чисел $\mathbb{Q}$.

В этом поле содержится элемент $[x]$, о котором можно сказать следующее:

$$[x]^2 = [x^2] = [x^2+1-1] = [-1] = -1$$

Поэтому, факторкольцо $\mathbb{Q}[x]/(x^2+1)$ вложить в $\mathbb{R}$ невозможно. Традиционно $[x]$ называют мнимой единицей и обозначают как i.

Гауссовы рациональные числа всегда можно привести к стандартному виду

$$a + ib, \quad a, b \in \mathbb{Q},$$

при этом a называют вещественной частью (real part) числа, b — мнимой (imaginary) частью. Sage всегда приводит элементы поля к этому стандартному виду:

```
sage: K.<ii>=QQ[x].quo(x^2+1)
sage: ii^2
-1
sage: K(x^3+2)
-ii + 2
sage: ii^3+2
-ii + 2
sage: ii^2+ii^3*2/(ii+1)
-ii - 2
```

Найти вещественную и мнимую части отдельно можно при помощи функции `list`:

```
sage: list(3*ii+2)
[2, 3]
sage: list(ii^2+ii^3*2/(ii+1))
[-2, -1]
```

7. Поле комплексных чисел

Поскольку x^2+1 не раскладывается на множители над $\mathbb{R}$, то есть поскольку мнимая единица i не принадлежит $\mathbb{R}$, факторкольцо $\mathbb{R}[x]/(x^2+1)$ является полем.

Определение 4. Факторкольцо $\mathbb{R}[x]/(x^2+1)$ называют полем комплексных чисел и обозначают как $\mathbb{C}$.

Элементами поля комплексных чисел будут множества многочленов

$$[f] = f + (x^2+1),$$

причем в качестве представителя класса $[f]$ берут остаток от деления f на x^2+1, то есть многочлен, степень которого строго меньше 2. Всякий элемент поля можно записать как

$$[a+bx] = [a] + i \cdot [b], \quad a, b \in \mathbb{R}$$

где $i = [x]$ — мнимая единица поля $\mathbb{C}$, то есть такой элемент, что $i^2 = -1$.

Множество всех комплексных чисел вида $[a]$, где $a \in \mathbb{R}$, изоморфно $\mathbb{R}$. Таким образом, поле комплексных чисел — расширение поля вещественных чисел:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Обычно комплексное число записывают без квадратных скобок как

$$a + ib, \quad a, b \in \mathbb{R}.$$

Эту форму считают стандартной, a называют вещественной частью (real part) числа, b — мнимой (imaginary) частью.

В Sage символ i зарезервирован за мнимой единицей, поэтому его не стоит переопределять.

```
sage: i=sqrt(-1)
sage: CC(3*i+2)
2.00000000000000 + 3.00000000000000*I
sage: CC(i^2+i^3*2/(i+1))
-2.00000000000000 - 1.00000000000000*I
sage: CC(1/i+i^2*pi)
-3.14159265358979 - 1.00000000000000*I
```

```
sage: CC(1/i+i^2*pi).real()
-3.14159265358979
sage: CC(1/i+i^2*pi).imag()
-1.00000000000000
```

Нетрудно заметить, что

$$a + ib = a' + ib'$$

верно тогда и только тогда, когда $a = a'$ и $b = b'$. В самом деле,

$$a + ib = a' + ib'$$

означает, что

$$[a + bx] = [a' + b'x]$$

или

$$a - a' + (a - b')x + (x^2 + 1) = 0$$

Это в свою очередь означает, что остаток от деления $a - a' + (a - b')x$ на $x^2 + 1$ равен нулю. Поскольку степень многочлена $a - a' + (a - b')x$ меньше 2, этот остаток равен $a - a' + (a - b')x$. Поэтому этот многочлен равен нулю, что означает равенство нулю его коэффициентов.

Сопоставим комплексному числу $a + ib$ точку (a, b) плоскости $\mathbb{R}^2$. Это соответствие — взаимно однозначное, поэтому $\mathbb{C}$ часто называют комплексной плоскостью. При этом числа $a + i0$ попадают на ось абсцисс, которую называют вещественной осью, а числа $0 + ib$ — на ординат, которую называют мнимой осью. Желая оторвать теорию комплексных чисел от теории факторколец, поле комплексных чисел описывают как множество точек плоскости $\mathbb{R}^2$, на котором введены арифметические действия

$$(a, b) + (a', b') = (a + a', b + b')$$

и

$$(a, b) \cdot (a', b') = (ab' - a'b, ab' + a'b)$$

Второе означает просто

$$(a+ib)(a'+ib') = aa' - bb' + (ab' + a'b)i.$$

При этом замечательным образом оказывается, что плоскость с так введенным арифметическими действиями является полем.

Следуя этой геометрической интерпретации комплексного числа, вводят модуль (или абсолютное значение) комплексного числа

$$|a+ib| = \sqrt{a^2+b^2}$$

и аргумент комплексного числа, то есть угол между вектором, проведенным из начала координат в точку (a, b) и положительным направлением вещественной оси.

```
sage: CC(1/i+i^2*pi).abs()
3.29690830947562
sage: CC(1/i+i^2*pi).arg()
-2.83342358247381
sage: tan(CC(1/i+i^2*pi).arg())
0.318309886183791
sage: CC(1/i+i^2*pi).imag()/CC(1/i+i^2*pi).real()
0.318309886183791
```

Символ i в символьном выражение трактуется как мнимая единица:

```
sage: real(1/i+3*i^2)
-3
sage: imag(1/i+3*i^2)
-1
sage: abs(1/i+3*i^2)
sqrt(10)
sage: arg(1/i+3*i^2)
-pi + arctan(1/3)
```

Теорема 4 (основная теорема алгебры)**.** Всякое уравнение из $\mathbb{C}[x]$ имеет хотя бы один комплексный корень.

Эта теорема давно уже не основная для алгебры, аккуратно она была доказана в первой половине XIX века, самое короткое доказательство получается из теоремы Лиувилля в теории функций комплексной переменной. В те же времена Грефе разработал итерационный метод для приближенного отыскания корней уравнения любой степени с комплексными коэффициентами. В Sage реализован такой алгоритм, что позволяет приближенно находить корни.

Пример 2. Найдем корни уравнения

$$x^5 + 2x + 3 = 0$$

и отметим их на комплексной плоскости. Корни найдем стандартным путем:

```
sage: f=ZZ[x](x^5+2*x+3)
sage: f.roots(CC)
[(-1.00000000000000, 1), (-0.578147130265194 -
  1.08949615540615*I, 1), (-0.578147130265194 +
  1.08949615540615*I, 1), (1.07814713026519 -
  0.899807460564854*I, 1), (1.07814713026519 +
  0.899807460564854*I, 1)]
```

Проверка:

```
sage: L=f.roots(CC)
sage: [abs(f.subs(x=L[n][0])) for n in range(len(L))
  ]
[0.000000000000000, 6.66133814775094e-16,
  6.66133814775094e-16, 1.11022302462516e-15,
  1.11022302462516e-15]
```

Чтобы нарисовать точки, создадим список этих точек:

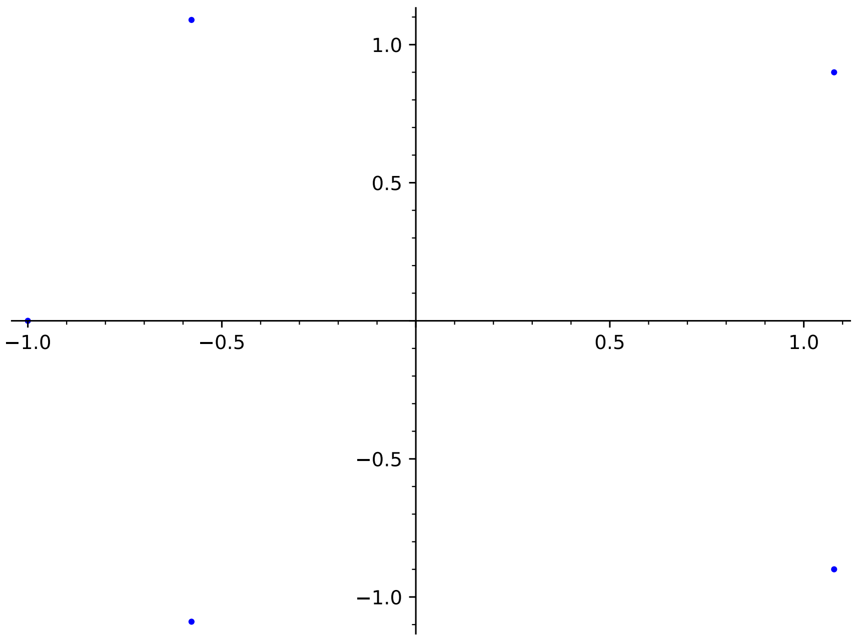

Рис. 1. Корни уравнения $x^5 + 2x + 3 = 0$ на комплексной плоскости

```
sage: P=[list(L[n][0]) for n in range(len(L))]
sage: P
[[-1.00000000000000, 0.000000000000000],
  [-0.578147130265194, -1.08949615540615],
  [-0.578147130265194, 1.08949615540615],
  [1.07814713026519, -0.899807460564854],
  [1.07814713026519, 0.899807460564854]]
```

Чтобы нарисовать эти точки воспользуемся функцией `point`, аргументом которой служит список точек:

```
sage: point(P)
Graphics object consisting of 1 graphics primitive
```

Результат представлен на рис. 1.

В численных методах обсуждается вопрос о том, на сколько отличается приближенное решение о точного. Мы лишь заметим, что результаты, которые выдает Sage без ворнингов, далеко не всегда отвечают ожиданиям юзера.

Пример 3. Найдем корни уравнения

$$\prod_{n=0}^{24}(x-n)=0$$

стандартным путем:

```
sage: ZZ[x](prod([x-n for n in range(25)])).roots(CC)
[(0.000000000000000, 1), (1.00000000000000, 1),
  (2.00000000000033, 1), (2.99999999978751, 1),
  (4.00000001616415, 1), (4.99999945269449, 1),
  (6.00001044842235, 1), (6.99987500877393, 1),
  (8.00099552907990, 1), (8.99465223136176, 1),
  (10.0202704556859, 1), (10.9557561298711, 1),
  (12.0295509619359, 1), (23.0376059919101, 1),
  (23.9967524278318, 1), (13.3132205646180 -
  0.233917803496413*I, 1), (13.3132205646180 +
  0.233917803496413*I, 1), (15.3130804708819 -
  0.970744064828818*I, 1), (15.3130804708819 +
  0.970744064828818*I, 1), (17.5094104316040 -
  1.18136339295327*I, 1), (17.5094104316040 +
  1.18136339295327*I, 1), (19.6912393268465 -
  0.934744654969230*I, 1), (19.6912393268465 +
  0.934744654969230*I, 1), (21.6553148792901 -
  0.248729024988977*I, 1), (21.6553148792901 +
  0.248729024988977*I, 1)]
```

Хорошо видно, что последние элементы списка не являются корнями даже близко. Поэтому мы настоятельно рекомендуем выполнять проверку.

8. Задания

Теоретические задания.

1) Дайте определение поля гауссовых рациональных чисел.

2) Дайте определение поля комплексных чисел.

3) Что такое вещественная и мнимая части комплексного числа?

4) Что такое модуль и аргумент комплексного числа?

5) Почему $\mathbb{Q}[x]/(x^2-2)$ вложено в $\mathbb{R}$, а $\mathbb{Q}[x]/(x^2+1)$ — нет?

Практические задания.

1) Приведите комплексные числа к стандартному виду

   а) $2i^2 - 1/i$

   б) $i^2/(i^3-2)^2$

   в) $(i+i^2)/(i+3i^2)+4i$

2) Нарисуйте число $i-1$ на комплексной плоскости. Найдите его модуль и аргумент.

3) Найдите корни нижеследующих уравнений в полях $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$. Нарисуйте их на комплексной плоскости.

   а) $x^2+5x=10$

   б) $x^2+5x+10=0$

   в) $x^3+5x+10=0$

   г) $x^4+5x+10=0$

   д) $x^5+5x+10=0$

4) Среди комплексных корней уравнения

$$x^5+2x+10=0$$

   выберете те, которые имеют наибольший модуль.