Кольца и идеалы

Основной объект изучения коммутативной алгебры – коммутативное кольцо.

Определение 1. *Коммутативным кольцом* называется множество A с заданными на нём операциями $+ \colon A \times A \to A$ (сложение) и $\cdot : A \times A \to A$ (умножение), удовлетворяющими следующим аксиомам:

1. $\forall a, b, c \in A \ (a+b)+c = a+(b+c)$ (ассоциативность сложения);
2. существует элемент $0 \in A$, для которого $\forall a \in A \ a+0 = 0+a = a$ (наличие нуля);
3. для любого $a \in A$ существует $b \in A$ (он обозначается $-a$), для которого $a+b = b+a = 0$ (наличие противоположного);
4. $\forall a, b \in A \ a+b = b+a$ (коммутативность сложения);

   первые четыре аксиомы означают, что A является коммутативной группой по сложению
5. $\forall a, b, c \in A \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность умножения);
6. существует элемент $1 \in A$, не равный 0, для которого $\forall a \in A \ a \cdot 1 = 1 \cdot a = a$ (наличие единицы);
7. $\forall a, b, c \in A \ (a+b) \cdot c = a \cdot c + b \cdot c$ и $a \cdot (b+c) = a \cdot b + a \cdot c$ (дистрибутивность умножения);

   первые семь аксиом означают, что A – это кольцо
8. $\forall a, b \in A \ a \cdot b = b \cdot a$ (коммутативность умножения).

В любом кольце ноль и единица единственны, также противоположный элемент к каждому элементу единствен.

Пример 2. Встречающиеся в природе примеры колец:

- Кольца чисел: целые, рациональные, действительные, комплексные, гауссовы, вида $a + b\sqrt{2}, a, b \in \mathbb{Z}$.
- Кольцо остатков: остатки от деления на фиксированное число $n \in \mathbb{N}, n \geqslant 2$, образуют кольцо, где операции – сложение и умножение по модулю n.
- Кольца многочленов: $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}[x], (\mathbb{Z}/n\mathbb{Z})[x], \ldots$, кольца многочленов от нескольких переменных $\mathbb{Q}[x_1, x_2, \ldots, x_n]$, $\mathbb{C}[x_1, x_2, \ldots, x_n]$.
- Кольца функций: все вещественные функции на множестве, непрерывные вещественные функции на отрезке, дифференцируемые функции на плоскости, гладкие функции на гладком многообразии, булевы функции на множестве, ...

Определение 3. Если в кольце дополнительно выполнена аксиома:

9. $\forall a \neq 0 \in A \ \ \exists b \in A \ \ ab = 1$,

то это кольцо называется *полем*.

Определение 4. Элементы $a, b \in A$ называются *делителями нуля*, если $a, b \neq 0$ и $ab = 0$.
Кольцо, в котором нет делителей нуля, называется *целостным*.

Пример 5. Остатки $[4], [6]$ – делители нуля в кольце $\mathbb{Z}/12\mathbb{Z}$, так как $[4] \cdot [6] = [0]$ в $\mathbb{Z}/12\mathbb{Z}$.

Задача 1. Найдите все делители нуля в $\mathbb{Z}/m\mathbb{Z}$.

Определение 6. *Прямым произведением колец* A и B называется теоретико-множественное прямое произведение $A \times B$ с покомпонентными операциями. Оно также является кольцом.

Пример 7. В прямом произведении колец всегда есть делители нуля: элементы $(0, 1)$ и $(1, 0)$.

Определение 8. Отображение колец $f\colon A \to B$ называется *изоморфизмом*, если оно взаимно-однозначно и при этом $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ для всех $a, b \in A$. Кольца называются *изоморфными*, если между ними существует изоморфизм.

Несложно видеть, что обратное отображение к изоморфизму – изоморфизм и композиция изоморфизмов – изоморфизм. Также легко проверить, что при изоморфизме ноль переходит в ноль, а единица переходит в единицу.

Пример 9. Кольца $\mathbb{Z}/6\mathbb{Z}$ и $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ изоморфны.
Изоморфизм $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ задаётся формулой $f([n]) = ([n], [n])$.

Пусть A – кольцо. Рассмотрим элементы $0, 1, 1 + 1, 1 + 1 + 1, \ldots$ и $-1, -(1 + 1), -(1 + 1 + 1), \ldots$ в A. Они также образуют кольцо. Если среди сумм вида $1 + 1 + \ldots + 1$ есть ноль, то это кольцо изоморфно кольцу $\mathbb{Z}/m\mathbb{Z}$, где m – наименьшее натуральное число, что $\underbrace{1 + 1 + \ldots + 1}_{m} = 0$. Если же все суммы $1 + 1 + \ldots + 1$ ненулевые, то это кольцо изоморфно кольцу целых чисел.

Если при этом A – поле, то число m простое. Оно называется *характеристикой* поля. Если в поле все суммы $\underbrace{1 + 1 + \ldots + 1}_{m}$ не равны нулю, то его характеристика считается равной нулю.

Таким образом, любое поле содержит либо поле $\mathbb{Z}/p\mathbb{Z}$, где p простое, либо кольцо $\mathbb{Z}$ (а значит, и поле $\mathbb{Q}$).

Задача 2 (Китайская теорема об остатках). Пусть m и n – взаимно простые числа. Докажите, что кольца $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ и $\mathbb{Z}/mn\mathbb{Z}$ изоморфны.

Подсказка: постройте отображение в какую-нибудь из сторон и проверьте, что это изоморфизм колец.

Задача 3. Опишите все изоморфизмы колец а) $\mathbb{Z}/n\mathbb{Z}$ и b^*) $\mathbb{R}$ на себя.

Определение 10. Подмножество $I \subset A$ называется *идеалом*, если оно содержит ноль, замкнуто относительно сложения и взятия обратного:

$$a, b \in I \Rightarrow a + b \in I,\ -a \in I$$

а также умножения на элементы из A:

$$a \in A, k \in I \Rightarrow ak \in I.$$

Заметим, что идеал является подгруппой по сложению. В любом кольце A есть два тривиальных идеала: $\{0\}$ и A. Если кольцо – поле, то других идеалов нет. Поэтому с точки зрения коммутативной алгебры поля – объекты сложности ноль.
Задача 4. Покажите, что кольцо есть поле $\Leftrightarrow$ все его идеалы тривиальны.

Пример 11. Найдём все идеалы в целых числах. Пусть $I \subset \mathbb{Z}$ и $I \neq 0$, пусть n – наименьший натуральный элемент в $\mathbb{Z}$. Тогда все числа вида kn также лежат в I. Покажем, что других чисел там нет. Действительно, пусть $m \in I$, поделим m на n с остатком: $m = nq + r$, причём $r \in I$. Если $r = 0$, то $m \vdots n$, иначе $0 < r < n$ и получим противоречие с минимальностью n.

Таким образом, все идеалы в $\mathbb{Z}$ имеют вид $(n) = \{kn \mid k \in \mathbb{Z}\}$, $n \in \mathbb{Z}$.

Пример 12. Пусть $p_1, \ldots, p_k \in A$ – элементы произвольного кольца. Тогда множество $\{f \in A[x] \mid f(p_1) = \ldots = f(p_k) = 0\}$ является идеалом в кольце многочленов $A[x]$.

Определение 13. *Главным идеалом* в кольце называется идеал вида $\{ka \mid k \in A\}$, где $a \in A$ – фиксированный элемент. Обозначение: (a).

Пример 14. Пример неглавного идеала: идеал многочленов, обращающихся в ноль в точке $(0, 0)$, в $\mathbb{C}[x, y]$. Он содержит x и y, которые не могут принадлежать одному главному идеалу.

Определение 15. Пусть $T \subset A$ – произвольное подмножество. *Идеал, порожденный набором элементов* T, – это по определению наименьший по вложению идеал, содержащий T. Обозначение: $\langle T \rangle$ или (T).

Задача 5. Покажите, что идеал, порождённый семейством элементов $T \subset A$, существует и состоит из всевозможных конечных сумм $\sum_i a_i t_i$, где $a_i \in A, T_i \in T$.

Определение 16. *Кольцом главных идеалов* называется кольцо, в котором любой идеал главный.

Задача 6. Пусть $e \in A$ – *идемпотент*, т.е. такой элемент, что $e^2 = e$.
a) Идеал (e) является кольцом относительно сложения и умножения из A.
b) Кольцо A изоморфно прямому произведению колец (e) и $(1 - e)$.

Предложение 17. *Пересечение идеалов – идеал.*

Определение 18. *Суммой* идеалов I и J кольца A называется множество элементов вида $i + j$, где $i \in I$, $j \in J$. Обозначение $I + J$.

Сумма идеалов является идеалом. Также можно определить сумму идеалов как идеал, порождённый множеством $I \cup J$.

Пример 19. Найдём пересечение и сумму идеалов в $\mathbb{Z}$. Идеал $(m) \cap (n)$ состоит из чисел, делящихся и на m, и на n, т.е, делящихся на НОК(m, n). Идеал $(m) + (n)$ состоит из чисел вида $am + bn$, то есть, чисел, делящихся на НОД(m, n). Итого

$$(m) \cap (n) = \text{НОК}(m, n), \qquad (m) + (n) = \text{НОК}(m, n).$$

Определение 20. Идеал называется *максимальным*, если он отличен от всего кольца и максимален по вложению среди всех таких идеалов. Идеал I называется *простым*, если для всех элементов $x, y \in A$ выполнено $xy \in I \Rightarrow x \in I$ или $y \in I$.

Пример 21. Найдём максимальные и простые идеалы в $\mathbb{Z}$. Максимальными будут идеалы (p) для простых p и только они, простыми идеалами будут они же и идеал (0).

Отметим важный факт: любой идеал можно вложить в максимальный. Доказать это строго, однако, не просто: для этого нужна аксиомы выбора (например, в форме леммы Цорна).

Пример 22. Идеал $(x) \subset \mathbb{C}[x, y]$ прост, но не максимален.

Предложение 23. *Любой максимальный идеал прост.*

Доказательство. Это сразу следует из (ещё не доказанных) предложений 26 и 27: ведь в поле нет делителей нуля. $\square$

Задача 7. Опишите простые и максимальные идеалы в $\mathbb{Z}/m\mathbb{Z}$.
Задача 8. Любой идеал в $A \times B$ имеет вид $I \times J$, где $I \subset A$ и $J \subset B$ – идеалы.
Задача 9. Любой простой идеал в $A \times B$ имеет вид $\mathfrak{p} \times B$ или $A \times \mathfrak{q}$, где $\mathfrak{p} \subset A$ и $\mathfrak{q} \subset B$ – простые идеалы.

Определение 24. Пусть $I \subset A$ – идеал, $I \neq A$. Множество классов эквивалентности элементов A по следующему отношению эквивалентности: $a \sim b$, если $a - b \in I$, обозначается A/I. Класс эквивалентности элемента a обозначим $[a]$. На множестве A/I определены сложение и умножение по формулам $[a] + [b] = [a + b]$, $[ab] = [a][b]$. Можно проверить, что эти операции определены корректно и превращают A/I в коммутативное кольцо. Оно называется *факторкольцом* кольца A по идеалу I.

Пример 25. Кольца остатков от деления на n – это факторкольцо кольца $\mathbb{Z}$ по идеалу (n).

Предложение 26. *Факторкольцо не имеет делителей нуля $\Leftrightarrow$ идеал прост.*

Доказательство. Очевидно: $xy \in I$ равносильно $[x][y] = [0]$, а $x \in I$ равносильно $[x] = [0]$. $\square$

Предложение 27. *Факторкольцо – поле $\Leftrightarrow$ идеал максимален.*

Доказательство. Пусть A/I – поле, и I не максимален, т.е. есть строго больший идеал: $I \subset J$. Возьмём $x \in J \setminus I$. Элемент $[x] \neq [0]$ в факторкольце, значит там существует обратный $[x][y] = [1]$, т.е. $xy - 1 = i \in I$. Получаем $1 = xy - i \in J$, и $J = A$. Противоречие.

Пусть I максимален и $[x] \neq [0]$ – элемент кольца A/I. Тогда $x \notin I$, значит идеал $I + (x)$ больше, чем I, и поэтому $I + (x) = A$. Значит, $i + kx = 1$ при некоторых $i \in I, k \in A$. Поэтому $[k][x] = [i] + [k][x] = [1]$ в A/I, и у $[x]$ есть обратный. $\square$

Задача 10. Найти факторкольцо $\mathbb{C}[x]/I$, где
a) $I = \{f \mid f(2) = 0\}$;
b) $I = \{f \mid f(2) = f(3) = f(-2) = 0\}$.

Особую роль в кольцах играют нильпотентные элементы, или нильпотенты.

Определение 28. Элемент $a \in A$ называется *нильпотентом*, если $a^n = 0$ при некотором $n \in \mathbb{N}$. *Нильрадикалом* кольца называется множество его нильпотентов. Обозначение: $\mathcal{N}(A)$.

Предложение 29. *Нильрадикал кольца есть идеал.*

Доказательство. Во-первых, надо проверить: если a и b нильпотенты, то $a \pm b$ нильпотент. Пусть $a^n = 0, b^m = 0$, тогда $(a \pm b)^{m+n} = 0$ по биному Ньютона. Во-вторых, пусть a – нильпотент, $a^n = 0$, тогда при любом $k \in A$ $(ka)^n = 0$ и ka – тоже нильпотент. $\square$

Пример 30. Нильрадикал в $\mathbb{Z}/8\mathbb{Z}$ – идеал, порождённый [2].

Задача 11. a) Нильрадикал $\mathbb{Z}/m\mathbb{Z}$ тривиален $\Leftrightarrow$ m свободно от квадратов.
b) Найдите нильрадикал $\mathbb{Z}/m\mathbb{Z}$ в общем случае.
Задача 12. Если n – нильпотент, то $1 + n$ – обратимый элемент.

Предложение 31. *Фактор по нильрадикалу имеет нулевой нильрадикал.*

Доказательство. Пусть $[a] \in \mathcal{N}(A/\mathcal{N}(A))$, тогда $[a]^n = [0]$ при некотором n. Значит $a^n \in \mathcal{N}(A)$, следовательно $(a^n)^m = 0$ при некотором m. Поэтому $a^{mn} = 0$, a – нильпотент и значит $[a] = [0]$. $\square$

Предложение 32. *Пересечение всех простых идеалов – нильрадикал.*

Доказательство. Проверим, что любой простой идеал содержит все нильпотенты. Действительно, для нильпотента a имеем $a^n = 0 \in I$. По определению простого идеала, если $a \notin I$, то $a^{n-1} \in I, a^{n-2} \in I, \ldots$ и так приходим к противоречию.

Включение в другую сторону мы проверим позднее. $\square$

Список литературы

[1] Атья М., Макдональд И., Введение в коммутативную алгебру

[2] Eisenbud D., Commutative algebra with a view toward algebraic geometry

[3] Шафаревич И. Р., Основы алгебраической геометрии

[4] Винберг Э. Б., Курс алгебры

[5] Зарисский О., Самюэль П., Коммутативная алгебра