

3. ТРЕТЬЯ ЛЕКЦИЯ, 20 СЕНТЯБРЯ 2021 г.

В предыдущей части курса рассматривались вопросы, связанные с делимостью, разложением на множители и т.д. в кольцах целых чисел и многочленов. Наша ближайшая задача — обобщить эти понятия на более широкий класс колец. Для начала напомним определение кольца.

3.1. Кольца, поля, идеалы.

Определение 3.1. *Кольцо* (точнее, коммутативное ассоциативное кольцо с единицей — пока что мы будем рассматривать только такие) — это множество A , снабжённое двумя бинарными операциями, сложением и умножением, удовлетворяющими следующим аксиомам:

- (A1): сложение коммутативно: $a + b = b + a$ для любых $a, b \in A$;
- (A2): сложение ассоциативно: $(a + b) + c = a + (b + c)$ для любых $a, b, c \in A$;
- (A3): существование нуля: существует такой элемент $0 \in A$, для которого $a + 0 = a$ для любого $a \in A$;
- (A4): существование обратного по сложению: для любого $a \in A$ существует такой элемент $-a \in A$, для которого $a + (-a) = 0$;
- (M1): умножение коммутативно: $ab = ba$ для любых $a, b \in A$;
- (M2): умножение ассоциативно: $a(bc) = (ab)c$ для любых $a, b, c \in A$;
- (M3): существование единицы: существует такой элемент $1 \in A$, для которого $1 \cdot a = a$ для любого $a \in A$;
- (D): дистрибутивность: $(a + b)c = ac + bc$.

Замечание 3.2. Мы не требуем того, что $1 \neq 0$. Однако если единица равна нулю, то кольцо A состоит только из нуля (докажите это!)

Замечание 3.3. Если в кольце $1 \neq 0$ и выполнена аксиома существования обратного по умножению:

- (M4): для любого ненулевого элемента $a \in A$ существует $a^{-1} \in A$, для которого $a \cdot a^{-1} = 1$,

то такое кольцо называется *полем*.

В дальнейшем буквой $\mathbb{K}$ (от немецкого Körper) мы без дополнительных оговорок будем называть произвольное поле.

Упражнение 3.4. Докажите, что в произвольном кольце:

- (1) ноль единственен;
- (2) единица единственна;
- (3) $0 \cdot a = 0$ для любого $a \in A$.

Кроме того, напомним определение обратимого элемента. Элемент $a \in A$ называется *обратимым*, если существует такой элемент $b \in A$, для которого $ab = 1$. Ясно, что произведение обратимых элементов обратимо; т.е. обратимые элементы образуют группу по умножению, которая обычно обозначается $A^\times$.

3.2. Целостные кольца.

Определение 3.5. Кольцо A называется *целостным* (другой термин: *область целостности*), если в нем произведение двух ненулевых элементов всегда отлично от нуля. Иными словами, если для $a, b \in A$ выполнено равенство $ab = 0$, то либо $a = 0$, либо $b = 0$.

Упражнение 3.6. Докажите, что всякое поле является целостным кольцом.

Примеры 3.7. Кольцо $\mathbb{Z}/m\mathbb{Z}$ является целостным (и даже является полем) тогда и только тогда, когда m просто.

Предложение 3.8. Пусть A — целостное кольцо. Тогда кольцо многочленов $A[x]$ также является целостным.

Доказательство. Предположим противное: пусть в $A[x]$ нашлись два многочлена $P(x) = a_n x^n + \dots$ и $Q(x) = b_m x^m + \dots$, для которых $P(x)Q(x) = 0$, причем a_n и b_m отличны от 0. Но тогда равен нулю и старший коэффициент произведения $P(x)Q(x) = a_n b_m x^{n+m} + \dots$, что противоречит целостности кольца A . $\square$

3.3. Идеалы.

Определение 3.9. Пусть A — произвольное кольцо. Подмножество $I \subset A$ называется *идеалом*, если выполнено следующее:

(I1): $\forall x, y \in I \ x + y \in I$;

(I2): $\forall x \in I \ -x \in I$;

(I3): $\forall x \in I, a \in A$ верно, что $ax \in I$.

Обратите внимание, что в третьей аксиоме требуется замкнутость I по умножению на все элементы из A (а не только из I) — это очень существенное ограничение.

В частности, если $I \ni 1$, то $I = A$: единицу можно умножить на любой элемент кольца, и результат будет снова принадлежать I . По той же причине идеал, содержащий любой *обратимый* элемент, совпадает со всем кольцом.

Приведем несколько примеров идеалов.

Пример 3.10. В любом кольце есть два тривиальных идеала: нулевой (состоящий из одного нуля) и всё кольцо. Впрочем, некоторые авторы предпочитают считать, что $I \neq A$, и всё кольцо, таким образом, идеалом не считается — но это вопрос терминологический.

Пример 3.11. Пусть $d \in \mathbb{Z}$. Множество $(d) = \{dm \mid m \in \mathbb{Z}\} \subset \mathbb{Z}$ является идеалом в $\mathbb{Z}$. Чуть позже мы проверим, что всякий идеал в $\mathbb{Z}$ имеет такой вид.

Пример 3.12. Пусть $a_1, \dots, a_m \in A$ — некоторое подмножество элементов кольца. Идеал, порожденный $a_1, \dots, a_m$, обозначается $(a_1, \dots, a_m)$. Это минимальный по включению идеал, содержащий эти элементы. Ясно, что он имеет вид

$$(a_1, \dots, a_m) = \{a_1 x_1 + \dots + a_m x_m \mid x_1, \dots, x_m \in A\}.$$

В предыдущем примере можно также взять любое подмножество в A , не обязательно конечное, и породить им идеал.

Вот ещё один пример, который оказывается очень важным в алгебраической геометрии.

Пример 3.13. Пусть $A = \mathbb{K}[x_1, \dots, x_n]$, и пусть $S \subset \mathbb{K}^n$ — произвольное подмножество точек в n -мерном аффинном пространстве. Множество функций, равных нулю во всех точках S , образует идеал в A .

3.4. Кольца главных идеалов.

Определение 3.14. Идеал вида $(a) \subset A$, т.е. порождённый одним элементом, называется *главным идеалом*.

Определение 3.15. Целостное кольцо A называется *кольцом главных идеалов*, если все идеалы в нём являются главными.

Предложение 3.16. $\mathbb{Z}$ и $\mathbb{K}[x]$ — кольца главных идеалов.

Доказательство. Пусть I — ненулевой идеал в $\mathbb{Z}$. Выберем в нём наименьший положительный элемент и обозначим его через d . Докажем, что $I = (d)$. Действительно, пусть $x \in I$. Разделим x на d с остатком: $x = dq + r$. Значит, $r = x - dq$. Оба слагаемых в правой части принадлежат I , значит, $r \in I$. Но $0 \leq r < d$. Поэтому $r = 0$, и x делится на d нацело. Значит, $x \in (d)$.

Случай $\mathbb{K}[x]$ разбирается аналогично, только в качестве d надо взять элемент наименьшей степени. $\square$

Упражнение 3.17. Докажите, что $\mathbb{Z}[x]$ и $\mathbb{K}[x, y]$ не являются кольцами главных идеалов.

Упражнение 3.18. Рассмотрим кольцо формальных степенных рядов $\mathbb{K}[[x]]$. Какие в нём существуют идеалы? Будет ли оно кольцом главных идеалов?

3.5. Евклидовы кольца. Неформально говоря, евклидовыми называются кольца, в которых возможно деление с остатком (т.е. алгоритм Евклида).

Определение 3.19. Целостное кольцо A называется *евклидовым*, если в нём существует функция *нормы*, или *высоты*,

$$n: A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0},$$

удовлетворяющая аксиомам:

(E1): $n(xy) \geq n(x)$ для любых $x, y \in A$;

(E2): Для любых $x, y \in A$, где $y \neq 0$, найдутся такие $q, r \in A$, что $x = qy + r$, причём либо $n(y) > n(r)$, либо $r = 0$.

Упражнение 3.20. Докажите, что аксиома (E1) на самом деле является избыточной: а именно, если на A существует функция, удовлетворяющая (E2), то из неё можно изготовить функцию (вообще говоря, другую), удовлетворяющую обоим аксиомам.

Примеры 3.21. Кольца $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[[x]]$ являются евклидовыми. Нормами в них являются соответственно модуль целого числа, степень многочлена и порядок нуля степенного ряда (т.е. номер первого ненулевого коэффициента).

Пример 3.22. Кольцо *целых гауссовых чисел* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ является евклидовым кольцом. Норма на нём задаётся как $n(a + bi) = a^2 + b^2$.

Предложение 3.23. *Всякое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Это доказывается аналогично предложению 3.16, при помощи выбора в идеале элемента наименьшей нормы. $\square$

Замечание 3.24. Бывают (достаточно экзотические) примеры колец главных идеалов, не являющихся евклидовыми. Таким, например, является кольцо $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Задача со звёздочкой: докажите это.

3.6. Делимость в кольцах главных идеалов. В этом разделе A — кольцо главных идеалов.

Дадим определение наибольшего общего делителя двух элементов. Привычное определение 1.2 здесь уже не работает, т.к. в произвольном кольце непонятно, что такое «наибольший». Поэтому придётся обобщать определение 1.3.

Определение 3.25. Пусть $a, b \in A$. *Наибольшим общим делителем* элементов a, b (обозначение: (a, b)) называется такой элемент d , что $d \mid a$ и $d \mid b$, и при этом d делится на *любой другой* общий делитель элементов a и b .

При таком определении а priori неясно, что НОД двух элементов вообще существует. Однако это несложно доказать.

Предложение 3.26. В кольце главных идеалов у любых двух элементов $a, b \in A$ существует наибольший общий делитель, который выражается через них в виде $d = ax + by$.

Доказательство. Рассмотрим идеал $(a, b) \subset A$. Он главный; пусть он порождён элементом d . Это значит, что $d = ax + by$. Докажем, что d — НОД элементов a и b . Действительно, поскольку $a, b \in (a, b) = (d)$, оба этих элемента делятся на d . Пусть e — какой-то другой общий делитель a и b . Поскольку $e \mid a$ и $e \mid b$, получаем, что $e \mid ax + by = d$, что и требовалось. $\square$

Определение 3.27. Если $(a, b) = 1$, то a и b называются *взаимно простыми*.

3.7. Существование и единственность разложения на простые. Введем понятие *ассоциированных* элементов. Два элемента a и b называются ассоциированными (обозначение: $a \sim b$), если $a = bs$, где s обратим. Иными словами, элементы a и b ассоциированы, если идеалы (a) и (b) совпадают.

Простое число — это такое число, которое делится на единицу и на себя. Обобщим это понятие на произвольные кольца.

Определение 3.28. Необратимый ненулевой элемент p кольца A называется *простым*, если его нельзя представить в виде $p = ab$, где a и b — необратимые элементы. Иными словами, всякий делитель простого элемента p ассоциирован либо с 1, либо с p .

Замечание 3.29. Простые элементы в кольце многочленов обычно называют *неприводимыми*.

Наша ближайшая цель — доказать существование и единственность разложения элемента в произведение простых в кольцах главных идеалов. Сначала докажем следующую лемму.

Лемма 3.30. Пусть A — кольцо главных идеалов, элемент p прост, и $p \mid a_1 \dots a_n$. Тогда $p \mid a_i$ при некотором i .

Доказательство. Сначала докажем лемму при $n = 2$. Пусть $p \mid ab$. Допустим, что $p \nmid a$; покажем, что $p \mid b$. Действительно, если p не делит a , то p и a взаимно просты. Напишем линейное выражение их НОДа:

$$1 = px + ay.$$

Домножим обе части равенства на b :

$$b = pbx + aby.$$

Правая часть делится на p , так как ab делится на p . Значит, b делится на p .

Случай произвольного n доказывается индукцией по числу сомножителей. $\square$

Отсюда следует единственность разложения элемента кольца главных идеалов на простые множители (с точностью до ассоциированности) — аналог основной теоремы арифметики. Доказательство в этом случае также почти не отличается от случая кольца целых чисел.

Теорема 3.31. Пусть A — кольцо главных идеалов, $a \in A$ — необратимый элемент, причём

$$a = p_1 \dots p_n = q_1 \dots q_m,$$

где p_i, q_i простые. Тогда $n = m$, причём $q_1, \dots, q_n$ можно перенумеровать так, что каждый из q_i станет ассоциированным с соответствующим p_i .

Доказательство. Пусть $n \leq m$. Докажем теорему индукцией по n . База: при $n = 1$ доказывать нечего.

Переход. Поскольку $p_1 \mid q_1 \dots q_m$, в силу предыдущей леммы p_1 делит некоторый q_i . Без ограничения общности будем считать, что $i = 1$. Поскольку q_1 также прост, получаем, что $p_1 \tilde{q}_1$. Стало быть, обе части равенства $p_1 \dots p_n = q_1 \dots q_m$ можно сократить на p_1 и получить равенство $p_2 \dots p_n = sq_2 \dots q_m$, где s обратим. Мы свели теорему к случаю $n - 1$ сомножителя, а для него она верна по предположению индукции. $\square$

Теперь докажем *существование* разложения элемента в произведение простых. Это утверждение, которое в $\mathbb{Z}$ очевидно, в случае произвольного кольца главных идеалов приходится доказывать. Кроме того, бывают кольца (не являющиеся кольцами главных идеалов), в которых разложения элемента в произведение простых не существует.

Теорема 3.32. *В кольце главных идеалов каждый ненулевой необратимый элемент может быть разложен на простые множители.*

Доказательство. Пусть это не так, и существуют элементы, которые не раскладываются в произведение простых. Назовём их *плохими*. Пусть a_0 — плохой элемент. Тогда он раскладывается в произведение двух необратимых элементов (иначе он был бы простым), причём хотя бы один из сомножителей обязан также быть плохим. Пусть $a_0 = a_1 b_1$, и a_1 плохой. То же самое верно про a_1 : он раскладывается в произведение $a_2 b_2$, где a_2 плохой, и так далее до бесконечности. Мы получили бесконечный ряд элементов

$$a_0, a_1, \dots, a_n, \dots,$$

где $a_i \mid a_{i-1}$. Поэтому имеет место бесконечная строго возрастающая цепочка идеалов

$$(a_0) \subset (a_1) \subset \dots \subset (a_n) \subset \dots$$

Докажем, что в кольце главных идеалов такой цепочки быть не может. Рассмотрим объединение всех идеалов цепочки: $I = \bigcup_{i=0}^{\infty} (a_i)$. Это тоже идеал (почему?). Пусть $I = (d)$ (ведь A — кольцо главных идеалов!). Тогда элемент d лежит в каком-то из (a_n) для некоторого n . Стало быть, $(a_n) = (a_{n+1}) = I$ — противоречие с тем, что цепочка строго возрастает. Стало быть, всякий элемент разлагается на простые множители. $\square$

Замечание 3.33. Это же рассуждение проходит для существенно более широкого класса колец: так называемых *нётеровых колец*, в которых каждый идеал конечно порождён. Поэтому в нётеровых кольцах имеет место существование разложения в произведение простых — а вот единственности там может и не быть.

Определение 3.34. Целостное кольцо, в котором каждый ненулевой необратимый элемент разлагается в произведение простых, причём единственным (в смысле теоремы 3.32) образом, называется *факториальным*.

Это определение позволяет объединить теоремы 3.32 и 3.31:

Теорема 3.35. *Всякое кольцо главных идеалов факториально.*