Алгебра, первый курс, четвертый модуль

Е. Ю. Смирнов

Аннотация. Записки лекций по алгебре для первого курса факультета математики ВШЭ, весна 2013/14 учебного года

1. Первая лекция, 2 апреля 2014 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 кольца́.

1.1. Кольца, поля, идеалы.

Определение 1.1. *Кольцо* — это множество A, снабжённое двумя бинарными операциями: *сложением* и *умножением*, удовлетворяющими следующим аксиомам:

(A1-A4): A является абелевой группой по сложению;
(D1): левая дистрибутивность: $a(b+c) = ab + ac$;
(D2): правая дистрибутивность: $(a+b)c = ac + bc$.

Определение 1.2. Коммутативное ассоциативное кольцо с единицей — это кольцо, операция умножения в котором удовлетворяет ещё трём дополнительным аксиомам:

(M1): коммутативность умножения: $ab = ba$ для любых $a, b \in A$;
(M2): ассоциативность умножения: $a(bc) = (ab)c$ для любых $a, b, c \in A$;
(M3): существование единицы: $\exists 1 \in A$: $\forall a \in A\ 1 \cdot a = a$;

В ближайших нескольких лекциях мы будем рассматривать только коммутативные ассоциативные кольца с единицей.

Замечание 1.3. Мы не требуем того, что $1 \neq 0$. Однако если единица равна нулю, то кольцо A состоит только из нуля (докажите это!)

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

Замечание 1.4. Если $1 \neq 0$ и выполнена аксиома существования обратного по умножению:

(M4): $\forall a \in A\ \exists a^{-1} \in A$: $a \cdot a^{-1} = 1$,

то такое кольцо называется *полем*.

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

Определение 1.5. 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 $ax \in I$.

Первые две аксиомы равносильны тому, что I — подгруппа в A по сложению (в частности, $0 \in I$). На самом деле вторая аксиома следует из третьей: т.к. $-1 \in A$, то I оказывается замкнуто по умножению на -1: то есть если $x \in I$, то $-x \in I$.

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 1.6. 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 1.7. 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 1.8. Пусть $a_1, \ldots, a_m \in A$ — некоторое подмножество элементов кольца. *Идеал, порожденный* $a_1, \ldots, a_m$, обозначается $(a_1, \ldots, a_m)$. Это минимальный по включению идеал, содержащий эти элементы. Ясно, что он имеет вид

$$(a_1, \ldots, a_m) = \{a_1x_1 + \cdots + a_mx_m \mid x_1 \ldots, x_m \in A\}.$$

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

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

Пример 1.9. Пусть $A = \mathbb{K}[x_1, \ldots, x_n]$, $S \subset \mathbb{K}^n$ — произвольное подмножество точек в n-мерном аффинном пространстве. Множество функций, равных нулю во всех точках S, образует идеал в A.

1.2. **Кольца главных идеалов.**

Определение 1.10. Идеал вида $(a) \subset A$, т.е. порождённый одним элементом, называется *главным идеалом*.

Определение 1.11. Кольцо называется *целостным* (или *областью целостности*), если в нём произведение любых двух ненулевых элементов отлично от нуля (т.е. из того, что $ab = 0$, следует, что либо $a = 0$, либо $b = 0$).

Определение 1.12. Целостное кольцо A называется *кольцом главных идеалов*, если все идеалы в нём являются главными.

Предложение 1.13. *$\mathbb{Z}$ 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. □

Упражнение 1.14. Докажите, что $\mathbb{Z}[x]$ и $\mathbb{K}[x, y]$ не являются кольцами главных идеалов.

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

Определение 1.15. Целостное кольцо A называется *евклидовым*, если в нём существует функция *нормы*, или *высоты*,

$$n\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0},$$

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 1.16. 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 обеим аксиомам.

Примеры 1.17. 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).

Предложение 1.18. *Всякое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Это доказывается аналогично предложению 1.13, при помощи выбора в идеале элемента наименьшей нормы. □

Замечание 1.19. 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.

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

Дадим определение наибольшего общего делителя двух элементов. Привычное определение придётся модифицировать, т.к. в произвольном кольце не совсем понятно, что такое "наибольший".

Определение 1.20. 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 a priori неясно, что НОД двух элементов вообще существует. Однако это несложно доказать.

Предложение 1.21. *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. □

Определение 1.22. Если $(a, b) = 1$, то a и b называются *взаимно простыми*.

1.5. **Существование и единственность разложения на простые.** Введем понятие *ассоциированных* элементов. Два элемента a и b называются ассоциированными (обозначение: $a\tilde{b}$), 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 1.23. 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 1.24. 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 1.25. *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 $p \not| a$; 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. □

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 1.26. *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 $p_2 \dots p_n = s q_2 \dots q_m$, где s обратим. Мы свели теорему к случаю $n - 1$ сомножителя, а для него она верна по предположению индукции. □

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 1.27. *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

$$a_0, a_1, \ldots, a_n, \ldots,$$

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

$$(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \ldots.$$

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. □

Замечание 1.28. 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 1.29. Целостное кольцо, в котором каждый ненулевой необратимый элемент разлагается в произведение простых, причём единственным (в смысле теоремы 1.27) образом, называется *факториальным*.

Это определение позволяет объединить теоремы 1.27 и 1.26:

Теорема 1.30. *Всякое кольцо главных идеалов факториально.*

1.6. **Факторкольца.** [1]

[1] Материал следующих двух параграфов изучался в первом семестре; на лекции было дано лишь краткое напоминание того, что такое факторкольцо, гомоморфизм и т.д. Здесь это изложено более развёрнуто.

Ранее мы рассматривали конструкцию факторгруппы по нормальной подгруппе. Для колец есть её непосредственный аналог: факторкольцо по идеалу.

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv y \mod I$, если $x - y \in I$. Ясно, что это отношение эквивалентности. Классы эквивалентности — это множества вида $x + I = \{x + a \mid a \in I\}$. Иногда мы также будем обозначать класс $x + I$ через $[x]$. Обозначим множество этих классов через A/I.

На классах эквивалентности из A/I можно определить операции сложения и умножения:

$$(x + I) + (y + I) = (x + y) + I; \qquad (x + I)(y + I) = xy + I.$$

Предложение 1.31. *Заданные таким образом операции определены корректно, т.е. сумма и произведение классов не зависят от выбора их представителей.*

Доказательство. Проверим корректность умножения: пусть $x \equiv x' \mod I$ и $y \equiv y' \mod I$. Тогда $x' = x' + a$, $y' = y + b$, где $a, b \in I$. Поэтому

$$x'y' = (x + a)(y + b) = xy + ay + xb + ab \equiv xy \mod I,$$

поскольку ay, xb и ab лежат в I. Корректность сложения проверяется аналогично. □

Таким образом, на A/I вводятся операции сложения и умножения, что задаёт на нём структуру кольца. Полученное кольцо называется *факторкольцом* кольца A по идеалу I.

Ясно, что нулём и единицей в A/I являются $0 + I$ и $1 + I$ соответственно.

Упражнение 1.32. Докажите утверждение, обратное к предыдущему предложению: пусть $I \subset A$ — абелева подгруппа по сложению, причем операция умножения, заданная на классах эквивалентности из A/I, определена корректно. Покажите, что I — идеал в A.

1.7. **Гомоморфизмы.**

Определение 1.33. Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Замечание 1.34. В определении мы *не требуем*, чтобы единица переходила в единицу. Так, например, вложение $A \to A \oplus A$, $a \mapsto (a, 0)$ — гомоморфизм, хотя единицу в единицу он не переводит.

Упражнение 1.35. Докажите, что $\operatorname{Im} f \subset B$ — подкольцо в B, а $\operatorname{Ker} f \subset A$ — идеал в A.

Говорят, что гомоморфизм инъективен/сюръективен/биективен, если он инъективен/сюръективен/биективен как отображение множеств. Такие гомоморфизмы ещё называют соответственно *мономорфизмами*, *эпиморфизмами* и *изоморфизмами*.

Пример 1.36. Важный пример гомоморфизма — отображение факторизации $\pi\colon A \to A/I$, $\pi(a) = a + I$, где I — произвольный идеал в кольце A. Ясно, что π — эпиморфизм.

Следующая теорема утверждает, что всякий эпиморфизм является отображением факторизации по некоторому идеалу. Аналоги этой теоремы для факторгрупп и факторпространств уже разбирались ранее.

Теорема 1.37 (о гомоморфизме колец)**.** *Пусть $f\colon A \to B$ — гомоморфизм колец. Тогда $\operatorname{Im} f \simeq A/\operatorname{Ker} f$. Более точно, отображение $\varphi\colon \operatorname{Im} f \to A/\operatorname{Ker} f$, при котором $b = f(a) \in \operatorname{Im} f$ отображается в $\pi(a) = a + \operatorname{Ker} f$, есть изоморфизм.*

Доказательство. Из теоремы о гомоморфизме групп следует, что отображение φ является изоморфизмом абелевых групп. Осталось проверить, что оно сохраняет умножение. Действительно, пусть $f(x) = u$, $f(y) = v$. Тогда $f(xy) = uv$, и

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v),$$

что и требовалось. □

Пример 1.38. Рассмотрим отображение

$$\varphi\colon \mathbb{K}[x] \to \mathbb{K}, \qquad f(x) \mapsto f(a)$$

вычисления значения многочлена в точке a. Ясно, что это гомоморфизм, причём сюръективный (значение многочлена в данной точке может быть любым). При этом по теореме Безу ядро φ есть

$$\operatorname{Ker} \varphi = \{f \in \mathbb{K}[x] \mid f(a) = 0\} = (x - a).$$

Значит, $\mathbb{K}[x]/(x - a) \cong \mathbb{K}$.

Пример 1.39. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i:

$$\mathbb{R}[x] \to \mathbb{C}, \qquad f(x) \mapsto f(i).$$

Это гомоморфизм, причем также сюръективный (проверьте это!). Кроме того, если $f(i) = 0$, то $f(-i) = f(\bar{i}) = \overline{f(i)} = 0$, поэтому $f(x) \vdots (x-i)(x+i) = x^2+1$. Значит,

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

Упражнение 1.40. Чему изоморфно факторкольцо $\mathbb{R}[x]/(x^2+px+q)$? (ответ зависит от знака дискриминанта квадратного трёхчлена).

1.8. **Китайская теорема об остатках.** Сначала напомним понятие прямой суммы колец.

Определение 1.41. *Прямая сумма* $A \oplus B$ колец A и B — это кольцо, элеменами которого являются пары (a, b), где $a \in A$, $b \in B$, а сложение и умножение задаются покомпонентно.

Заметим, что подкольца $\{(a, 0)\} \cong A$ и $\{(0, b)\} \cong B$ являются идеалами в $A \oplus B$.

Вернёмся к кольцам главных идеалов. В них также имеет место аналог китайской теоремы об остатках, который очень просто формулируется и доказывается с помощью понятия факторкольца.

Теорема 1.42 (Китайская теорема об остатках)**.** *Пусть A — кольцо главных идеалов, элементы $u, v \in A$ взаимно просты. Тогда*

$$A/(uv) \simeq A/(u) \oplus A/(v).$$

Доказательство. Поскольку u и v взаимно просты, через них можно линейно выразить единицу:

$$1 = au + bv.$$

Рассмотрим гомоморфизм

$$f\colon A \to A/(u) \oplus A/(v), \qquad f(x) = (x + (u), x + (v)).$$

Тогда $f(bv) = f(1-au) = (1, 0)$, $f(au) = f(1-bv) = (0, 1)$. Следовательно, гомоморфизм f сюръективен. Очевидно, что его ядро — это идеал (uv). Поэтому требуемое утверждение следует из теоремы о гомоморфизме колец. □

E-mail address: esmirnov@hse.ru