Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 7

Евклидовы кольца, кольца главных идеалов и факториальные кольца. Факториальность кольца многочленов от многих переменных.

В этой лекции всюду предполагается, что R — коммутативное кольцо без делителей нуля.

Определение 1. Говорят, что элемент $b \in R$ *делит* элемент $a \in R$ (b — *делитель* a, a *делится* на b; пишут $b \,|\, a$) если существует элемент $c \in R$, для которого $a = bc$.

Определение 2. Два элемента $a, b \in R$ называются *ассоциированными*, если $a = bc$ для некоторого обратимого элемента c кольца R.

Замечание 1. Легко видеть, что отношение ассоциированности является отношением эквивалентности на кольце R.

Определение 3. Кольцо R без делителей нуля, не являющееся полем, называется *евклидовым*, если существует функция

$$N \colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$$

(называемая *нормой*), удовлетворяющая следующим условиям:

1) $N(ab) \geqslant N(a)$ для всех $a, b \in R \setminus \{0\}$;

2) для любых $a, b \in R$, $b \neq 0$, существуют такие $q, r \in R$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Неформально говоря, условие 2) означает возможность «деления с остатком» в кольце R.

Примеры евклидовых колец:

1) $\mathbb{Z}$ с нормой $N(a) = |a|$;

2) $K[x]$ (где K — произвольное поле) с нормой $N(f) = \deg f$.

Лемма 1. *Пусть R — евклидово кольцо и $a, b \in R \setminus \{0\}$. Равенство $N(ab) = N(a)$ выполнено тогда и только тогда, когда b обратим.*

Доказательство. Если b обратим, то $N(a) \leqslant N(ab) \leqslant N(abb^{-1}) = N(a)$, откуда $N(ab) = N(a)$.

Пусть теперь $N(ab) = N(a)$. Разделим a на ab с остатком: $a = qab + r$, где либо $r = 0$, либо $N(r) < N(ab)$. Если $r \neq 0$, то с учётом равенства $r = a(1 - qb)$ имеем $N(a) \leqslant N(a(1 - qb)) = N(r) < N(ab) = N(a)$ — противоречие. Значит, $r = 0$ и $a = qab$, откуда $a(1 - qb) = 0$. Так как в R нет делителей нуля и $a \neq 0$, то $1 - qb = 0$, откуда $qb = 1$, т. е. b обратим. □

Определение 4. *Наибольшим общим делителем* элементов a и b кольца R называется их общий делитель, который делится на любой другой их общий делитель. Он обозначается (a, b).

Замечание 2. Если наибольший общий делитель двух элементов $a, b \in R$ существует, то он определён однозначно с точностью до ассоциированности, т. е. умножения на обратимый элемент кольца R.

Теорема 1. *Пусть R — евклидово кольцо и a, b — произвольные элементы. Тогда:*

(1) *существует наибольший общий делитель (a, b);*

(2) *существуют такие элементы $u, v \in R$, что $(a, b) = ua + vb$.*

Доказательство. В основе доказательства лежит следующее простое наблюдение: множество общих делителей элементов $a, b \in R$ совпадает с множеством общих делителей элементов $a - qb$ и b, где $q \in R$ — произвольный элемент. Отсюда вытекает, что $(a, b) = (b, a - qb)$.

Теперь доказательство утверждения (1) получается применением (прямого хода) алгоритма Евклида, а утверждения (2) — применением обратного хода в алгоритме Евклида. □

Определение 5. Кольцо R называется *кольцом главных идеалов*, если всякий идеал в R является главным.

Теорема 2. *Всякое евклидово кольцо R является кольцом главных идеалов.*

Доказательство. Пусть I — произвольный идеал в R. Если $I = \{0\}$, то $I = (0)$ и поэтому I является главным. Далее считаем, что $I \neq \{0\}$. Пусть $a \in I \setminus \{0\}$ — элемент с наименьшей нормой. Тогда главный идеал (a) содержится в I. Предположим, что какой-то элемент $b \in I$ не лежит в (a), т. е. не делится на a. Тогда разделим b на a с остатком: $b = qa + r$, где $r \neq 0$ и $N(r) < N(a)$. Так как $r = b - aq$, то $r \in I$, что в силу неравенства $N(r) < N(a)$ противоречит нашему выбору элемента a. □

Определение 6. Ненулевой необратимый элемент p кольца R называется *простым*, если он не может быть представлен в виде $p = ab$, где $a, b \in R$ — необратимые элементы.

Замечание 3. Простые элементы в кольце многочленов $K[x]$ над полем K принято называть *неприводимыми многочленами.*

Лемма 2. *Если простой элемент p евклидова кольца R делит произведение $a_1 a_2 \dots a_n$, то он делит один из сомножителей.*

Доказательство. Индукция по n. Пусть $n = 2$ и предположим, что p не делит a_1. Тогда $(p, a_1) = 1$ и по утверждению (2) теоремы 1 найдутся такие элементы $u, v \in R$, что $1 = up + va_1$. Умножая обе части этого равенства на a_2, получаем

$$a_2 = upa_2 + va_1a_2.$$

Легко видеть, что p делит правую часть последнего равенства, поэтому p делит и левую часть, т. е. a_2.

При $n > 2$ применяем предыдущее рассуждение к $(a_1 \dots a_{n-1})a_n$ и пользуемся предположением индукции. □

Определение 7. Кольцо R называется *факториальным*, если всякий его ненулевой необратимый элемент «разложим на простые множители», т. е. представим в виде произведения (конечного числа) простых элементов, причём это представление единственно с точностью до перестановки множителей и ассоциированности.

Более формально единственность разложения на простые множители следует понимать так: если для элемента $a \in R$ есть два представления

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

где все элементы p_i, q_j простые, то $n = m$ и существует такая подстановка $\sigma \in S_n$, что для каждого $i = 1, \dots, n$ элементы p_i и $q_{\sigma(i)}$ ассоциированы.

Теорема 3. *Всякое евклидово кольцо R является факториальным.*

Доказательство состоит из двух шагов.

Шаг 1. Сначала докажем, что всякий ненулевой необратимый элемент из R разложим на простые множители. Предположим, что это не так, и среди всех элементов, не разложимых на простые множители, выберем элемент a с наименьшей нормой. Тогда a не может быть простым (иначе он разложим в произведение, состоящее из одного простого множителя), поэтому существует представление вида $a = bc$, где $b, c \in R$ — ненулевые необратимые элементы. Но тогда в силу леммы 1 имеем $N(b) < N(a)$ и $N(c) < N(a)$, поэтому элементы b и c разложимы на простые множители. Но тогда и a разложим — противоречие.

Шаг 2. Докажем теперь индукцией по n, что если для некоторого элемента $a \in R$ имеются два разложения

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

где все элемнты p_i и q_j простые, то $m = n$ и после подходящей перенумерации элементов q_j окажется, что при всех $i = 1, \dots, n$ элемент p_i ассоциирован с q_i.

Если $n = 1$, то $a = p_1$; тогда из определения простого элемента следует, что $m = 1$ и тем самым $q_1 = p_1$. Пусть теперь $n > 1$. Тогда элемент p_1 делит произведение $q_1 q_2 \dots q_m$. По лемме 2 этот элемент делит некоторый q_i, а значит, ассоциирован с ним. Выполнив перенумерацию, можно считать, что $i = 1$ и $q_1 = cp_1$ для некоторого обратимого элемента $c \in R$. Так как в R нет делителей нуля, то мы можем сократить на p_1, после чего получится равенство

$$p_2 p_3 \dots p_n = (cq_2)q_3 \dots q_m$$

(заметьте, что элемент cq_2 прост!). Дальше используем предположение индукции. □

Можно показать (см. листок с задачами к лекции 6), что при $n \geqslant 2$ кольцо многочленов $K[x_1, \ldots, x_n]$ над произвольным полем K не является кольцом главных идеалов, а значит, по теореме 2 это кольцо не является евклидовым. Тем не менее, наша цель в оставшейся части этой лекции — доказать, что кольцо $K[x_1, \ldots, x_n]$ факториально.

Начнём издалека. С каждым (коммутативным) кольцом R (без делителей нуля) связано его *поле отношений* K. Элементами этого поля являются дроби вида $\frac{a}{b}$, где $a, b \in R$ и $b \neq 0$, со стандартными правилами отождествления ($\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$), сложения ($\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$) и умножения ($\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$). Кольцо R реализуется как подкольцо в K, состоящее из всех дробей вида $\frac{a}{1}$.

Модельный пример: $\mathbb{Q}$ есть поле отношений кольца $\mathbb{Z}$.

Всякий гомоморфизм колец $\varphi\colon R \to R'$ индуцирует гомоморфизм $\widetilde{\varphi}\colon R[x] \to R'[x]$ соответствующих колец многочленов, задаваемый по правилу

$$a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 \mapsto \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \ldots \varphi(a_1)x + \varphi(a_0).$$

Вспомнив, как определяется умножение в кольце многочленов, легко показать, что $\widetilde{\varphi}$ действительно является гомоморфизмом.

В частности, если R — кольцо и K — его поле частных, то вложение $R \hookrightarrow K$ индуцирует вложение $R[x] \hookrightarrow K[x]$, так что всякий многочлен с коэффициентами из R можно рассматривать как многочлен с коэффициентами из K.

Пусть R — кольцо.

Определение 8. Многочлен $f(x) \in R[x]$ называется *примитивным*, если в R нет необратимого элемента, который делит все коэффициенты многочлена $f(x)$.

Лемма Гаусса. Если R — факториальное кольцо с полем отношений K и многочлен $f(x) \in R[x]$ разлагается в произведение двух многочленов в кольце $K[x]$, то он разлагается в произведение двух пропорциональных им многочленов в кольце $R[x]$.

В доказательстве леммы Гаусса нам потребуются следующие факты.

Упражнение 1. Пусть R — факториальное кольцо и $p \in R$ — простой элемент. Тогда в факторкольце $R/(p)$ нет делителей нуля.

Упражнение 2. Пусть R — (коммутативное) кольцо (без делителей нуля). Тогда в кольце многочленов $R[x]$ также нет делителей нуля.

Доказательство леммы Гаусса. Пусть $f(x) = g(x)h(x)$, где $g(x), h(x) \in K[x]$. Так как кольцо R факториально, то для любого набора элементов из R определены наибольший общий делитель и наименьшее общее кратное. С учётом этого приведём все коэффициенты многочлена $g(x)$ к общему знаменателю, после чего вынесем за скобку этот общий знаменатель и наибольший общий делитель всех числителей. В результате в скобках останется примитивный многочлен $g_1(x) \in R[x]$, а за скобками — некоторый элемент из поля K. Аналогичным образом найдём примитивный многочлен $h_1(x) \in R[x]$, который пропорционален многочлену $h(x)$. Теперь мы можем записать $f(x) = \frac{u}{v}g_1(x)h_1(x)$, где $u, v \in R$, $v \neq 0$ и без ограничения общности можно считать $(u, v) = 1$. Для завершения доказательства достаточно показать, что элемент v обратим (и тогда разложение $f(x) = (uv^{-1}g_1(x))h_1(x)$ будет искомым).

Предположим, что v необратим. Тогда найдётся простой элемент $p \in R$, который делит v. Рассмотрим гомоморфизм факторизации $\varphi\colon R \to R/(p)$, $a \mapsto a + (p)$, и соответствующий ему гомоморфизм колец многочленов $\widetilde{\varphi}\colon R[x] \to (R/(p))[x]$. В кольце $R[x]$ у нас имеется равенство $vf(x) = ug_1(x)h_1(x)$. Взяв образ обеих частей этого равенства при гомоморфизме $\widetilde{\varphi}$, мы получим следующее равенство в кольце $(R/(p))[x]$:

$$\widetilde{\varphi}(v)\widetilde{\varphi}(f(x)) = \widetilde{\varphi}(u)\widetilde{\varphi}(g_1(x))\widetilde{\varphi}(h_1(x)). \tag{1}$$

Поскольку p делит v, имеем $\widetilde{\varphi}(v) = 0$, поэтому левая часть равенства (1) равна нулю. С другой стороны, из условия $(u, v) = 1$ следует, что $\widetilde{\varphi}(u) \neq 0$, а из примитивности многочленов $g_1(x)$ и $h_1(x)$ вытекает, что $\widetilde{\varphi}(g_1(x)) \neq 0$ и $\widetilde{\varphi}(h_1(x)) \neq 0$. Таким образом, все три множителя в правой части равенства (1) отличны от нуля. Из упражнений 1 и 2 вытекает, что в кольце $(R/(p))[x]$ нет делителей нуля, поэтому правая часть равенства (1) отлична от нуля, и мы пришли к противоречию. □

Следствие 1. *Если многочлен $f(x) \in R[x]$ может быть разложен в произведение двух многочленов меньшей степени в кольце $K[x]$, то он может быть разложен и в произведение двух многочленов меньшей степени в кольце $R[x]$.*

Теорема 4. *Если кольцо R факториально, то кольцо многочленов $R[x]$ также факториально.*

Доказательство. Следствие 1 показывает, что простые элементы кольца $R[x]$ — это в точности элементы одного из следующих двух типов:

1) простые элементы кольца R (рассматриваемые как многочлены степени 0 в $R[x]$);

2) примитивные многочлены из $R[x]$, неприводимые над полем отношений K.

Ясно, что каждый многочлен из $R[x]$ разлагается в произведение таких многочленов. Предположим, что какой-то элемент из $R[x]$ двумя способами представим в виде такого произведения:

$$a_1 \dots a_n b_1(x) \dots b_m(x) = a'_1 \dots a'_k b'_1(x) \dots b'_l(x),$$

где a_i, a'_j — простые элементы типа 1 и $b_i(x), b'_j(x)$ — простые элементы типа 2.

Рассмотрим эти разложения в кольце $K[x]$. Как мы уже знаем из теоремы 3, кольцо $K[x]$ факториально. Отсюда следует, что $m = l$ и после подходящей перенумерации элементов $b'_j(x)$ получается, что при всех $j = 1, \dots, m$ элементы $b_j(x)$ и $b'_j(x)$ ассоциированы в $K[x]$, а в силу примитивности они ассоциированы и в $R[x]$. После сокращения всех таких элементов у нас останутся два разложения на простые множители (какого-то) элемента из R. Но кольцо R факториально, поэтому эти два разложения совпадают с точностью до перестановки множителей и ассоциированности. □

Теорема 5. *Пусть K — произвольное поле. Тогда кольцо многочленов $K[x_1, \dots, x_n]$ факториально.*

Доказательство. Воспользуемся индукцией по n. При $n = 1$ наше кольцо евклидово и по теореме 3 факториально. При $n > 1$ имеем $K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n]$, кольцо $K[x_1, \dots, x_{n-1}]$ факториально по предположению индукции и требуемый результат следует из предыдущей теоремы. □

Замечание 4. Несмотря на естественность условия единственности разложения на простые множители, большинство колец не являются факториальными. Например, таковым не является кольцо $\mathbb{Z}[\sqrt{-5}]$, состоящее из всех комплексных чисел вида $a + b\sqrt{-5}$, где $a, b \in \mathbb{Z}$: в этом кольце число 6 разлагается на простые множители двумя различными способами: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 3, § 5, 10 и глава 9, § 5)

[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 5, § 2,3,4)

[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 4, § 2)

[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 14, § 63–64)