

8. Восьмая лекция, 14 февраля 2018 г.

Эта и следующая лекции посвящены строению конечнопорожденных модулей над евклидовыми кольцами. Практически все изложенные результаты имеют место и для произвольных колец главных идеалов. Основные идеи доказательств также остаются неизменными, отличие состоит лишь в незначительных технических деталях. Заинтересованный читатель может прочесть подробности в любом учебнике, например, у Винберга или Гроденцева.

8.1. Евклидовы кольца: сводка результатов. Напомним основные определения и факты, касающиеся евклидовых колец.

ОПРЕДЕЛЕНИЕ 8.1. Целостное коммутативное ассоциативное кольцо с единицей A называется *евклидовым*, если на нем введена функция $n: A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$, обладающая следующими свойствами:

- (1) $n(ab) \leq n(a)n(b)$ для любых ненулевых $a, b \in A$ (субмультипликативность);
- (2) для любых ненулевых $a, b \in A$ найдутся такие $q, r \in A$, что $a = bq + r$ и либо $n(r) < n(b)$, либо $r = 0$ (деление с остатком).

ПРИМЕР 8.2. Кольцо $\mathbb{Z}$ евклидово, $n(a) = |a|$.

ПРИМЕР 8.3. Кольцо многочленов над полем $\mathbb{K}[x]$ евклидово, норма — степень многочлена.

ПРИМЕР 8.4. Кольцо целых гауссовых чисел $\mathbb{Z}[i]$ евклидово, $n(a + bi) = a^2 + b^2$.

Далее через A будет обозначаться евклидово кольцо.

ПРЕДЛОЖЕНИЕ 8.5. Кольцо A является кольцом главных идеалов.

ДОКАЗАТЕЛЬСТВО. Рассмотрим идеал $I \subset A$ и докажем, что он главный. Пусть $d \in I$ — элемент наименьшей нормы. Тогда любой другой элемент $a \in A$ делится на d нацело: иначе бы получилось, что $a = dq + r$, где $r \in I$ и $n(r) < n(d)$ — противоречие с минимальностью. Значит, $I = (d)$. $\square$

СЛЕДСТВИЕ 8.6. Для любых $a, b \in A$ наибольший общий делитель $d = (a, b)$ линейно выражается через a и b : найдутся такие x, y , для которых $ax + by = d$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим идеал (a, b) . Он главный; его образующая d и будет НОДом a и b . Поскольку она лежит в идеале (a, b) , она линейно выражается через a и b . $\square$

СЛЕДСТВИЕ 8.7. Всякое евклидово кольцо факториально. Иначе говоря, любой его элемент обладает разложением на неприводимые множители, определенные однозначно с точностью до порядка и умножения на обратимые элементы.

ДОКАЗАТЕЛЬСТВО. См. первый семестр. $\square$

ПРЕДЛОЖЕНИЕ 8.8. *Элемент $p \in A$ неприводим тогда и только тогда, когда $A/(p)$ является полем.*

ДОКАЗАТЕЛЬСТВО. Пусть $p \in A$ неприводим. Возьмем произвольный $a \in A$, не делящийся на p , и покажем, что его класс $\bar{a} \in A/(p)$ обратим. В силу неприводимости p его НОД с a равен 1. Запишем линейное выражение НОД: $ax + py = 1$. Тогда, приведя это равенство по модулю идеала (p) , получим: $\bar{a}\bar{x} = \bar{1}$, то есть x — обратный к a . Все переходы были равносильными, что доказывает обратное утверждение. $\square$

ЗАМЕЧАНИЕ 8.9. Это утверждение верно для любого кольца главных идеалов. Однако для произвольных факториальных колец оно неверно: в них можно утверждать только то, что (p) будет областью целостности. Пример: $\mathbb{K}[x, y]/(x) \cong \mathbb{K}[y]$, а это, конечно же, не поле.

Еще одно утверждение о кольцах главных идеалов мы далее будем использовать постоянно.

ТЕОРЕМА 8.10 (китайская теорема об остатках). *Пусть $a, b \in A$ взаимно просты. Тогда $A/(ab) \cong A/(a) \oplus A/(b)$.*

8.2. Свободные модули над евклидовыми кольцами. Начиная с этого раздела все модули будут считаться конечнопорожденными, если не указано иное. Кольцо A — евклидово.

Итак, пусть L — конечнопорожденный A -модуль. В прошлой лекции мы увидели, что тогда $L \cong A^{\oplus r}$, где $r = \text{rk } L$ — ранг модуля.

Оказывается, что подмодуль свободного модуля также оказывается свободным. Более точно, верна следующая

ТЕОРЕМА 8.11. *Пусть M — свободный модуль, $\text{rk } M = m$, а $N \subset M$ — подмодуль. Тогда N также свободен, причем $\text{rk } N \leq \text{rk } M$.*

ДОКАЗАТЕЛЬСТВО. Индукция по рангу M . База индукции: если $\text{rk } M = 1$, то $M \cong A$, и подмодуль $N \subset A$ — это идеал. Но любой идеал является главным, поэтому $N = (d) \cong A$ (здесь мы существенно используем то, что A — кольцо главных идеалов!).

Переход. отождествим M с $A^{\oplus m}$. Рассмотрим множество $I \subset A$ всех первых координат элементов из N (т.е. множество таких x_1 , для которых найдется элемент $(x_1, \dots, x_m) \in N$). Очевидно, это идеал в A . Он порожден некоторым элементом $d \in A$.

Если $d = 0$, то N можно считать подмодулем в $A^{\oplus m-1}$ — у всех элементов N первая координата равна нулю. Поэтому по предположению индукции N свободен и $\text{rk } N \leq m - 1 < m$.

Если же $d \neq 0$, то возьмем элемент $x = (d, x_2, \dots, x_m)$, первая координата которого равна образующей идеала I . Рассмотрим подмодуль $N' = \{(0, x_2, \dots, x_m) \in N\} \subset N$. Это подмодуль в $A^{\oplus m-1}$, и по предположению индукции N' свободен. Далее, любой элемент N представляется единственным образом как сумма некоторого кратного x и элемента из N' , то есть $N = \langle x \rangle \oplus N'$. Стало быть, N свободен как прямая сумма двух свободных модулей, и $\text{rk } N = \text{rk } N' + 1 \leq m - 1 + 1 = m$. $\square$

8.3. Теорема о взаимных базисах. Хорошо известен следующий факт линейной алгебры: в паре $U \subset V$ из подпространства и пространства можно выбрать согласованный базис — т.е. такой базис $v_1, \dots, v_m$, что первые несколько векторов $v_1, \dots, v_n$ являются базисом U (здесь $n = \dim U \leq \dim V = m$). Ясно, что для модулей на это надеяться не приходится: даже в модуле ранга 1 бывают подмодули ранга 1, не совпадающие с ним. Однако аналогичное утверждение будет верным, если потребовать, чтобы базис подмодуля был бы образован не первыми из векторов базиса модуля, а *кратными* им элементами. Это и есть

ТЕОРЕМА 8.12 (о взаимных базисах). Пусть M — свободный модуль ранга m , $N \subset M$ — его подмодуль ранга $n \leq m$. Тогда существуют базисы $v_1, \dots, v_m$ в M , $u_1, \dots, u_n$ в N , для которых $u_i = d_i v_i$ при $i \leq n$, причем $d_i \nmid d_{i+1}$ при $1 \leq i < n$.

ДОКАЗАТЕЛЬСТВО. Возьмем произвольные базисы $u_1, \dots, u_n$ в N и $v_1, \dots, v_m$ в M . Представим u_i в виде линейных комбинаций v_j ; у нас получится матрица размера $n \times m$:

$$\begin{aligned} u_1 &= x_{11}v_1 + x_{12}v_2 + \dots + x_{1m}v_m, \\ &\dots \\ u_n &= x_{n1}v_1 + x_{n2}v_2 + \dots + x_{nm}v_m. \end{aligned}$$

Если наши базисы являются взаимными (т.е. такими, как в условии теоремы), то все элементы этой матрицы, кроме элементов вида x_{ii} , равны нулю. Если нет, то ее надо привести к такому виду, меняя базисы в M и N . Это можно делать при помощи процедуры, очень похожей на метод Гаусса.

Будем выполнять над строками этой матрицы элементарные преобразования трех типов:

- (1) прибавление к i -й строке j -й, умноженной на произвольный элемент кольца A ;
- (2) перестановка двух строк;
- (3) умножение строки на *обратимый* элемент кольца A .

При выполнении таких операций мы меняем базис подмодуля N , но сам подмодуль (т.е. множество всех линейных комбинаций базисных элементов) остается неизменным.

Такие же операции можно выполнять и над столбцами; при этом мы меняем базис самого модуля M .

Докажем, что при помощи таких операций можно привести матрицу к диагональному виду, причем для диагональных элементов $d_i = x_{ii}$ будет верно, что $d_i \mid d_{i+1}$.

Будем доказывать это убывающей индукцией по евклидовой норме элемента x_{11} . Для начала найдем элемент матрицы с минимальной нормой и поставим его в левый верхний угол при помощи преобразований второго типа.

Далее посмотрим на первый столбец. Если в нем имеется какой-нибудь элемент x_{i1} , не делящийся на x_{11} , то поделим его на x_{11} с остатком: $x_{i1} = x_{11}q + r$, и вычтем из i -й строки первую, умноженную на q . Далее поменяем i -ю строку местами с первой; в результате норма углового элемента уменьшится.

Будем повторять эту операцию; очередной шаг ее будет невозможен, если все элементы первого столбца будут делиться на x_{11} .

Когда это произойдет, будем делать то же самое со столбцами. Мы добьемся того, что все элементы первой строки будут делиться на (новый) элемент x_{11} . Однако при этом может «сломаться» делимость в первом столбце. Тогда снова перейдем к преобразованиям строк, и так далее. На каждом шаге норма углового элемента будет уменьшаться — то есть процесс в какой-то момент оборвется. Это произойдет тогда, когда все элементы и первой строки, и первого столбца будут делиться на x_{11} .

После этого найдем элемент x_{ij} , $i, j > 1$, не делящийся на x_{11} . Если такой есть, сделаем элемент x_{1j} равным нулю, вычтя из j -го столбца подходящее кратное первого, а потом прибавим j -й столбец к первому — от этого x_{11} не изменится, а x_{i1} перестанет делиться на x_{11} . Далее повторим всю процедуру сначала; это позволит уменьшить норму углового элемента.

Повторяя эти действия требуемое число раз, мы получим, что в итоге все элементы матрицы будут делиться на x_{11} . Когда это будет так, сделаем все элементы в первом столбце и первой строке нулями; получим матрицу вида

$$\begin{pmatrix} x_{11} & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{pmatrix},$$

в которой все элементы, отмеченные звездочками, делятся на $x_{11} = d$.

Дальше те же действия можно применить к подматрице, состоящей из звездочек, и т.д. В итоге получим диагональную матрицу, в которой каждый диагональный элемент x_{ii} будет делить $x_{i+1,i+1}$. Получившиеся в итоге замен базисы и будут искомыми. $\square$

ОПРЕДЕЛЕНИЕ 8.13. Полученный вид матрицы называется *нормальной формой Смита*, а элементы $d_1, \dots, d_n$ — *инвариантными множителями*.

ЗАДАЧА 8.14. Покажите, что для любого $1 \leq i \leq n$ наибольший общий делитель миноров i -го порядка матрицы (x_{ij}) равняется $d_1 \dots d_i$ (с точностью до умножения на обратимый элемент). В частности, d_1 — это наибольший общий делитель самих матричных элементов. Тем самым будет показано, что $d_1, \dots, d_n$ определены однозначно и не зависят от того, как именно мы приводили матрицу к нормальной форме Смита.