7. Седьмая лекция, 23 октября 2021 г.

Основная цель этой лекции — доказать теорему о факториальности кольца многочленов над факториальным кольцом. Ход доказательства очень похож на доказательство той же теоремы для кольца $\mathbb{Z}[x]$, разобранное в лекции 5 (теорема 5.19).

Для этого нам сначала понадобится ввести две технические конструкции: во-первых, доказать существование наибольшего общего делителя элементов в произвольном факториальном кольце. Во-вторых, мы введем конструкцию поля частных (поля отношений) данного целостного кольца: эта конструкция будет обобщать построение рациональных чисел с помощью целых.

7.1. **Наибольший общий делитель в факториальном кольце.** Пусть A — произвольное факториальное кольцо. Напомним, что наибольшим общим делителем (НОД) двух элементов $x, y \in A$ называется такой элемент $z \in A$, который, во-первых, делит x и y, а во-вторых, для любого w, делящего x и y, элемент w делит z.

Вообще говоря, существование такого элемента надо доказывать. В кольцах главных идеалов это следовало из того, что идеал (x, y) порожден одним элементом (это и есть их НОД); для факториальных колец доказазательство в каком-то смысле проще и ближе к тому, как НОД определялся в школьном курсе алгебры.

Предложение 7.1. *Для любых двух элементов факториального кольца A их НОД существует и единственен с точностью до умножения на обратимый элемент кольца.*

Доказательство. Единственность очевидна: если существуют два НОДа, значит, они делят друг друга, т.е. отличаются на обратимый множитель. Докажем существование.

Рассмотрим два элемента x, y. Разложим их на неприводимые множители. Пусть

$$x = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$
$$y = c p_1^{\ell_1} p_2^{\ell_2} \dots p_r^{\ell_r},$$

где p_i неприводимы, а $k_i, \ell_i \geq 0$ (равенство нулю отвечает случаю, когда p_i в разложение не входит).

Ясно, что элемент $z = p_1^{m_1} \dots p_r^{m_r}$ делит x (соответственно y) тогда и только тогда, когда $m_i \leq k_i$ (соответственно $m_i \leq \ell_i$) при всех i, не превосходящих r. Поэтому НОД элементов x и y имеет вид

$$w = p_1^{\min(k_1, \ell_1)} \dots p_r^{\min(k_r, \ell_r)}.$$

Такой элемент делит x и y, и в то же время всякий элемент, делящий x и y, делит и w. □

7.2. **Поле частных.** При доказательстве теоремы о факториальности $\mathbb{Z}[x]$ мы вкладывали кольцо $\mathbb{Z}$ в поле рациональных чисел $\mathbb{Q}$. Обобщим эту конструкцию на произвольное целостное кольцо.

Итак, пусть A — произвольное целостное кольцо. Рассмотрим множество пар

$$A \times (A \setminus \{0\}) = \{(a, b) \mid a, b \in A, b \neq 0\}.$$

Введем на этом множестве отношение:

$$(a, b) \sim (a', b'), \quad \text{если} \quad ab' = a'b.$$

Легко проверить, что это отношение будет отношением эквивалентности (проделайте это). Обозначим фактормножество по этому отношению эквивалентности через $\operatorname{Quot} A$.

Введем на $\operatorname{Quot} A$ операции сложения, умножения и взятия обратного по правилу:

$$(a,b)+(c,d)=(ad+bc,bd), \qquad (a,b)\cdot(c,d)=(ac,bd), \qquad (a,b)^{-1}=(b,a).$$

Кроме того, определим вложение $A \hookrightarrow \operatorname{Quot} A$, переводящее a в $(a,1)$. Это, в частности, задаст нам в $\operatorname{Quot} A$ нуль $(0,1)$ и единицу $(1,1)$.

Упражнение 7.2. Покажите, что операции сложения, умножения и взятия обратного корректно определены на фактормножестве $\operatorname{Quot} A$, и что они превращают $\operatorname{Quot} A$ в поле.

Определение 7.3. Множество $\operatorname{Quot} A$ называется *полем частных* (или *полем отношений*) кольца A.

Ясно, что первый и второй элементы пары (a,b) следует воспринимать как числитель и знаменатель дроби; тогда определенные выше операции как раз отвечают операциям с дробями.

Примеры 7.4. Поле частных кольца $\mathbb{Z}$ — это рациональные числа $\mathbb{Q}$. Поле частных кольца многочленов $\mathbb{K}[x]$ называется *полем рациональных функций* и обозначается через $\mathbb{K}(x)$.

Упражнение 7.5. Покажите, что поле частных кольца формальных степенных рядов $\mathbb{K}[[x]]$ есть поле *рядов Лорана* $\mathbb{K}[[x,x^{-1}]]$ (количество ненулевых коэффициентов при отрицательных степенях x в таких рядах конечно).

7.3. **Факториальность кольца многочленов над факториальным кольцом.** В этом разделе мы докажем следующую теорему.

Теорема 7.6. *Пусть A — факториальное кольцо. Тогда и кольцо многочленов $A[x]$ тоже факториально.*

Из этой теоремы моментально получается полезное следствие.

Следствие 7.7. *Кольцо многочленов от нескольких переменных $A[x_1,\dots,x_n]$ факториально.*

Доказательство теоремы 7.6 в основном повторяет ход доказательства теоремы 5.19. Поэтому ряд подробностей в доказательстве мы опустим.

Доказательство теоремы 7.6. Пусть $f(x)\in A[x]$. Как и для целочисленного случая, определим *содержание* $\operatorname{cont} f \in A$ многочлена f как НОД его коэффициентов.

Лемма 7.8 (Гаусс)**.** *Содержание мультипликативно:*

$$\operatorname{cont} fg = \operatorname{cont} f \cdot \operatorname{cont} g.$$

Доказательство. Достаточно доказать, что если $\operatorname{cont} f = \operatorname{cont} g = 1$, то и $\operatorname{cont} fg = 1$. Предположим, что $\operatorname{cont} fg \vdots p$, где p — некоторый неприводимый элемент. Это значит, что кольцо $B = A/(p)$ целостное. Рассмотрим эпиморфизм факторизации $A \to B$; он продолжается до эпиморфизма колец многочленов $A[x] \to B[x]$; последнее кольцо также будет целостным. Получаем, что $\overline{fg} \in B[x]$ равняется нулю (все коэффициенты этого многочлена делятся на p). Но многочлены f и g примитивны, т.е. их образы $\overline{f}$ и $\overline{g}$ отличны от нуля; противоречие с неприводимостью. $\square$

Далее обозначим через $Q = \operatorname{Quot} A$ поле частных кольца A. Заметим, что кольцо $Q[x]$ — это кольцо многочленов над полем от одной переменной, т.е. оно евклидово, а значит, факториально.

Аналогично следствию 5.18 можно доказать такое утверждение:

Следствие 7.9. *Если многочлен $f(x) \in A[x]$ раскладывается на неприводимые сомножители как многочлен из $Q[x]$, то он раскладывается на неприводимые сомножители той же степени с коэффициентами из $A[x]$.*

Тем самым мы получаем классификацию неприводимых элементов над $A[x]$: это, во-первых, примитивные многочлены, неприводимые над $Q[x]$, а во-вторых, неприводимые элементы из A (т.е. многочлены нулевой степени). Теорема доказана. □

7.4. **Определитель Вандермонда.** Факториальность кольца многочленов от нескольких переменных — очень полезное утверждение. Вычислим с его помощью *определитель Вандермонда.*

Предложение 7.10. *Имеет место равенство*

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Сначала докажем следующую лемму (полезную и саму по себе).

Лемма 7.11. *Пусть $f(x_1, \dots, x_n)$ — многочлен, тождественно обращающийся в нуль на гиперплоскости $a_1x_1 + \dots + a_nx_n = 0$. Тогда $f(x)$ делится на линейную форму $\ell(x) = a_1x_1 + \dots + a_nx_n$.*

Доказательство. Сделаем замену координат, при которой $\ell(x)$ перейдет в x_1. Представим многочлен $f(x)$ в виде $x_1g(x) + h(x)$. По условию, многочлен $f(x)$ тождественно равен 0 при $x_1 = 0$. Это значит, что $h(x) \equiv 0$, а значит, $f(x)$ делится на x_1, что и требовалось. □

Доказательство предложения 7.10. Обозначим определитель в левой части через $V(x) = V(x_1, \dots, x_n)$. Заметим, что при $x_i = x_j$ определитель $V(x)$ обращается в нуль как имеющий два одинаковых столбца. Значит, $V(x)$ делится на $x_j - x_i$. Но все двучлены $x_j - x_i$ попарно взаимно просты; значит, $V(x)$ делится и на их произведение, т.е. на правую часть равенства.

Далее, посмотрим на степень $V(x)$ как многочлена от $x_1, \dots, x_n$. Эта степень равна $0 + 1 + 2 + \dots + (n-1) = \frac{n(n-1)}{2}$. Но этому же равна и степень правой части: это количество пар (i, j), в которых $i < j$, т.е. $\binom{n}{2} = \frac{n(n-1)}{2}$. Значит, частное от деления левой части на правую является константой.

Осталось вычислить эту константу, вернее, показать, что она равна 1. Для этого вычислим константы при мономе $x_2x_3^2 \dots x_n^{n-1}$ в каждом из этих многочленов. В правой части она равна 1, т.к. такой моном получается при взятии переменной с большим номером из каждой скобки в произведении. В левой же части она получается из взятия диагональных элементов определителя, т.е. тоже равна 1. Предложение доказано. □

Упражнение 7.12. Докажите предложение 7.10, вычислив определитель в левой части с помощью элементарных преобразований строк.