

20. Двадцатая лекция, 4 апреля 2018 г.

20.1. Факториальность кольца многочленов. Лемма Гаусса. Наша ближайшая цель — доказать теорему о единственности разложения на множители для многочленов от нескольких переменных. Единственность разложения на множители для многочленов от одной переменной нам уже известна; она вытекает из евклидовости кольца $\mathbb{K}[x]$.

В этой лекции через A будет обозначаться целостное (т.е. без делителей нуля) коммутативное кольцо с единицей.

Напомним, что необратимый ненулевой элемент a кольца A называется *неприводимым*, если из равенства $a = bc$ вытекает, что либо b , либо c — обратимый элемент кольца A .

ОПРЕДЕЛЕНИЕ 20.1. Кольцо A называется *факториальным*, если каждый его необратимый ненулевой элемент раскладывается на неприводимые множители, причём это разложение единственно с точностью до перестановки сомножителей и умножения их на обратимые элементы кольца A .

Мы уже знаем, что всякое кольцо главных идеалов (в частности, $\mathbb{Z}$ и $K[x]$) факториально. Как мы увидим чуть ниже, обратное неверно: существуют факториальные кольца, не являющиеся кольцами главных идеалов.

В факториальном кольце для любых двух элементов можно рассмотреть их наибольший общий делитель. А именно, пусть

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k},$$

где p_i — неприводимые элементы кольца A , а $n_i, m_i \in \mathbb{Z}_{\geq 0}$. Тогда

$$(a, b) = p_1^{\min(n_1, m_1)} \dots p_k^{\min(n_k, m_k)}.$$

Элементы a и b называются *взаимно простыми*, если $(a, b) = 1$, то есть в разложениях a и b на неприводимые множители нет общих сомножителей.

ПРИМЕР 20.2. Кольцо $\mathbb{Z}[\sqrt{5}]$ не факториально. Действительно,

$$4 = 2 \cdot 2 = (\sqrt{5} + 1)(\sqrt{5} - 1)$$

— два различных разложения его элемента на неприводимые множители. (Проверьте самостоятельно, что ни один из них не обратим).

УПРАЖНЕНИЕ 20.3. Докажите, что кольцо $\mathbb{K}[x, y, z, t]/(xy - zt)$ не является факториальным.

ТЕОРЕМА 20.4. Пусть A — факториальное кольцо. Тогда кольцо многочленов $A[x]$ тоже факториально.

СЛЕДСТВИЕ 20.5. Кольца многочленов от нескольких переменных $\mathbb{Z}[x_1, \dots, x_n]$ и $K[x_1, \dots, x_n]$ факториальны.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Назовём многочлен $f(x) \in A[x]$ *примитивным*, если его коэффициенты взаимно просты в совокупности.

Пусть $\mathbb{K}$ — поле частных кольца A . Очевидно, что каждый многочлен можно представить в виде

$$h(x) = \frac{a}{b} h_0(x),$$

где $a, b \in A$ взаимно просты, а $h(x)$ — примитивный многочлен.

ЛЕММА 20.6 (лемма Гаусса). *Если многочлен $f(x)$ делится на примитивный многочлен $g(x)$ в кольце $\mathbb{K}[x]$, то он делится на него и в кольце $A[x]$ (т.е. все коэффициенты отношения этих многочленов принадлежат кольцу A).*

Примитивность здесь существенна: скажем, многочлен $x^2 - 1$ делится на многочлен $2x + 2$ (не являющийся примитивным) в кольце $\mathbb{Q}[x]$, однако, очевидно, не делится на него в $\mathbb{Z}[x]$.

Для доказательства нам потребуется следующая

ЛЕММА 20.7. *Пусть кольцо A факториально, $p \in A$ — неприводимый элемент. Тогда $A/(p)$ — область целостности.*

ДОКАЗАТЕЛЬСТВО. Предположим, что для каких-то двух элементов $a, b \in A$ их классы в $A/(p)$ в произведении дают нуль: $[a] \cdot [b] = 0 \pmod{(p)}$. Это значит, что ab делится на p . Но в силу факториальности кольца A это значит, что либо a , либо b делится на p , то есть либо $[a]$, либо $[b]$ сравним с нулем по модулю (p) . А это и есть определение целостного кольца. $\square$

ОПРЕДЕЛЕНИЕ 20.8. Идеал $\mathfrak{p}$, для которого $A/\mathfrak{p}$ есть область целостности, называется *простым*. Эквивалентное определение: идеал $\mathfrak{p}$ прост, если из $ab \in \mathfrak{p}$ следует, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Элемент $p \in A$ называется *простым*, если идеал (p) прост.

ЗАМЕЧАНИЕ 20.9. Очевидно, что каждый простой элемент неприводим. Лемма 20.7 утверждает, что в факториальных кольцах верно и обратное. Пример 20.2 показывает, что условие факториальности кольца A при этом существенно: так, в $\mathbb{Z}[\sqrt{5}]$ элемент 2 неприводим, но не прост: действительно, элементы $\sqrt{5} \pm 1$ не лежат в идеале (2) , тогда как их произведение там лежит.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ ГАУССА. Пусть $f(x) = g(x)h(x)$, где $h(x)$ примитивен. Представим $h(x)$ как $\frac{a}{b}h_0(x)$ и покажем, что b — обратимый элемент в кольце A .

Для этого используем редукцию по простому модулю. Пусть p — какой-то простой делитель элемента b . Умножим равенство $f(x) = \frac{a}{b}g(x)h_0(x)$ на b и произведем редукцию $A \rightarrow A/(p)$:

$$0 = [a]_p [g(x)]_p [h_0(x)]_p.$$

Все множители в правой части отличны от нуля: если бы $g(x)$ или $h_0(x)$ равнялись бы нулю в $A/(p)$, это значило бы, что все их коэффициенты делятся на p , что противоречит примитивности. Однако факторкольцо $A/(p)$ является целостным в силу леммы 20.7 — противоречие. $\square$

СЛЕДСТВИЕ 20.10. *Если многочлен $f(x) \in A[x]$ раскладывается в произведение двух многочленов меньшей степени над $\mathbb{K}[x]$, то он может быть разложен в произведение двух многочленов меньшей степени и над $A[x]$.*

УПРАЖНЕНИЕ 20.11. Завершите доказательство теоремы 20.4. $\square$

Ясно, что всякий многочлен первой степени неприводим.

Докажем следующую полезную лемму.

ЛЕММА 20.12. *Если многочлен $f(x) \in K[x_1, \dots, x_n]$ обращается в нуль во всех точках гиперплоскости $H_\ell = \{(x_1, \dots, x_n) \mid \ell(x) = a_1x_1 + \dots + a_nx_n = 0\}$, то он делится на ℓ .*

ДОКАЗАТЕЛЬСТВО. Сделав аффинную замену переменных, можем считать, что $\ell = x_1$. Тогда условие леммы означает, что все мономы многочлена $f(x)$ содержат x_1 , а значит, $f(x)$ делится на ℓ . $\square$

С помощью этой леммы и факториальности кольца многочленов можно, например, вычислить другим способом определитель Вандермонда.

ПРИМЕР 20.13. Пусть $\Delta(x_1, \dots, x_n) = \det(x_i^{j-1})_{i,j=1}^n$. Это многочлен от $x_1, \dots, x_n$ степени $n(n-1)/2$. Из свойств определителя следует, что он обращается в нуль при $x_i = x_j$, значит, в силу предыдущей леммы, он делится на $x_i - x_j$. Все эти многочлены неприводимы, значит, в силу факториальности, $\Delta(x_1, \dots, x_n)$ делится и на их произведение $\prod_{i>j}(x_i - x_j)$. Сравнивая степени, получаем, что коэффициент пропорциональности — константа. Вычислив коэффициент при каком-нибудь мономе (скажем, $x_2 x_3^2 \dots x_n^{n-1}$), получаем, что эта константа равна единице. Поэтому

$$\Delta(x_1, \dots, x_n) = \prod_{i>j}(x_i - x_j).$$