

17. Семнадцатая лекция, 2 апреля 2019 г.

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 $K[x]$.

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

17.1. Поле частных. Сначала напомним конструкцию *поля частных* (целостного коммутативного) кольца. Рассмотрим множество пар (a, b) , где $a, b \in A$, $b \neq 0$. отождествим пары (a, b) и (a', b') , если $ab' = a'b$. Полученное фактормножество обозначим через $\text{Quot } A$.

Введем на $\text{Quot } A$ операции сложения, умножения и взятия обратного по стандартным правилам (рассматривая (a, b) как «дробь» с числителем a и знаменателем b):

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

УПРАЖНЕНИЕ 17.1. Выполните все необходимые проверки корректности и покажите, что $\text{Quot } A$ является полем.

Имеется инъективный гомоморфизм колец $A \hookrightarrow \text{Quot } A$, $a \mapsto (a, 1)$. Ясно, что $\text{Quot } A$ — наименьшее поле, в которое вкладывается кольцо A .

ПРИМЕР 17.2. Из целых чисел в результате конструкции поля частных получаются рациональные числа: $\text{Quot } \mathbb{Z} = \mathbb{Q}$.

17.2. Факториальность кольца многочленов. Лемма Гаусса. 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 17.3. 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 $\mathbb{K}[x]$) 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 — простые 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 простые множители нет общих сомножителей.

УПРАЖНЕНИЕ 17.4. Докажите, что кольцо $\mathbb{K}[x, y, z, t]/(xy = zt)$ не является факториальным.

ТЕОРЕМА 17.5. Пусть A — факториальное кольцо. Тогда кольцо многочленов $A[x]$ тоже факториально.

СЛЕДСТВИЕ 17.6. Кольца многочленов от нескольких переменных $\mathbb{Z}[x_1, \dots, x_n]$ и $\mathbb{K}[x_1, \dots, x_n]$ факториальны.

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

Пусть Q — 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 17.7 (лемма Гаусса). *Если многочлен $f(x)$ делится на примитивный многочлен $g(x)$ в кольце $Q[x]$, 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 $Q[x]$, однако, очевидно, не делится на него в $Z[x]$.

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 неприводимый делитель элемента b . Соответствующий главный идеал $(p) \subset A$ будет прост, то есть $A/(p)$ будет областью целостности. 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 по простому идеалу является целостным — противоречие. $\square$

СЛЕДСТВИЕ 17.8. *Если многочлен $f(x) \in A[x]$ раскладывается в произведение двух многочленов меньшей степени над $Q[x]$, то он может быть разложен в произведение двух многочленов меньшей степени и над $A[x]$.*

Завершим доказательство теоремы. Рассмотрим произвольный многочлен $f(x) \in A[x]$. Разложим его на неприводимые множители в $Q[x]$:

$$f(x) = p_1(x) \dots p_r(x),$$

причем это разложение однозначно (в силу факториальности кольца $Q[x]$).

Согласно лемме Гаусса, существуют такие примитивные многочлены $\tilde{p}_i(x) \in A[x]$, пропорциональные соответствующим $p_i(x)$, для которых $f(x) = x\tilde{p}_1(x) \dots \tilde{p}_r(x)$. Коэффициент $c \in A$ является наибольшим общим делителем коэффициентов многочлена $f(x)$. Этот коэффициент однозначно разлагается на неприводимые в кольце A . Каждый из многочленов $\tilde{p}_i(x)$ определен однозначно и неприводим в $A[x]$ (т.к. неприводим в $Q[x]$ и примитивен). Теорема доказана. $\square$

Следующее полезное следствие описывает все неприводимые многочлены в $A[x]$.

СЛЕДСТВИЕ 17.9. *Всякий неприводимый элемент из $A[x]$ — это либо неприводимая константа из A , либо примитивный многочлен из $A[x]$, который остается неприводимым в кольце $Q[x]$.*

17.3. Признак неприводимости многочленов. Приведем теорему, которая позволяет доказывать неприводимость многочленов (над Z , хотя тот же результат дословно переносится на любое факториальное кольцо). Эта теорема обычно называется *критерием Эйзенштейна*, хотя это в строгом смысле не критерий (т.е. не утверждение «тогда и только тогда»), а лишь достаточное условие.

ТЕОРЕМА 17.10. *Рассмотрим примитивный многочлен $f(x) \in Z[x]$, $f(x) = a_n x^n + \dots + a_1 x + a_0$, причем существует такое простое число p , для которого:*

- p не делит a_n ;
- p делит все коэффициенты a_i при $0 \leq i < n$;
- a_0 не делится на p^2 .

Тогда многочлен $f(x)$ неприводим над $\mathbb{Z}[x]$.

ДОКАЗАТЕЛЬСТВО. Предположим противное: пусть $f(x) = g(x)h(x)$. Приведем это равенство по модулю p . Тогда $\bar{f}(x) = a_n x^n$. В силу однозначности разложения многочлена на множители получаем, что $\bar{g}(x) = c \cdot x^m$ и $\bar{h}(x) = c' \cdot x^{n-m}$, причем $m \neq 0, n$. То есть получается, что свободные члены $g(x)$ и $h(x)$ делятся на p , а значит, свободный член многочлена $f(x)$ делится на p^2 — противоречие. $\square$

ПРИМЕР 17.11. Докажем с помощью критерия Эйзенштейна неприводимость *циклотомического многочлена* (также называемого *многочленом деления круга*)

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x^2 + x + 1.$$

при простом p .

Сделаем замену $y = x - 1$. Тогда

$$\frac{x^p - 1}{x - 1} = \frac{(y + 1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \dots + \binom{p}{p-2} y + p,$$

и этот многочлен неприводим по критерию Эйзенштейна, т.к. $\binom{p}{k}$ делится на p при любом простом p и $0 < k < p$.

E-mail address: `esmirnov@hse.ru`