19 Факториальность кольца многочленов над факториальным кольцом

Пусть R – факториальное кольцо. Для $a, b \in R$ $a, b \neq 0$ определим наибольший общий делитель $(a, b) = c$ как

- $c \mid a$, $c \mid b$;
- если $d \mid a$, $d \mid b$, то $d \mid c$.

Лемма. *В факториальном кольце НОД существует и единственен с точностью до умножения на обратимый элемент.*

Доказательство. Выпишем разложения в произведения неразложимых:

$$a = up_1^{m_1} \cdots p_r^{m_r}, \qquad b = vp_1^{l_1} \cdots p_r^{l_r},$$

где m_i, $l_i \geq 0$, u, v – обратимые элементы и элементы $p_1, \ldots, p_r$ попарно неассоциированы. Положим $k_i = \min(l_i, m_i)$ и $(a, b) = p_1^{k_1} \cdots p_r^{k_r}$. □

Лемма. *Пусть R – факториальное кольцо, $p \in R$ – неразложимый элемент. Если $p \mid ab$, то $p \mid a$ или $p \mid b$.*

Доказательство. Разложим a и b как выше. Тогда

$$ab = uvp_1^{m_1+l_1} \cdots p_r^{m_r+l_r}.$$

С другой стороны,

$$ab/p = wq_1^{s1} \cdots q_r^{se} \implies ab = wpq_1^{s1} \cdots q_r^{se}.$$

Поэтому p ассоциирован с одним из p_i. □

Теорема. *Пусть R – факториальное кольцо. Тогда кольцо $R[t]$ факториально.*

Следствие. *Пусть F – поле. Кольца $F[t_1, \cdots, t_n]$ и $\mathbb{Z}[t_1, \cdots, t_n]$ факториальны.*

Пусть $F := \mathrm{Frac}(R)$. Многочлен $f = a_n t^n + \cdots + a_0 \in R[t]$ называется примитивным, если $(a_n, \ldots, a_0) = 1$.

Лемма. *Любой многочлен $f \in F[t]$ представляется в виде $f = \frac{\alpha}{\beta} f^*$, где $\alpha, \beta \in R$, $b \neq 0$, $f^* \in R[t]$ – примитивный многочлен.*

Доказательство. Пусть $f = a_n t^n + \cdots + a_0$, где $a_i = b_i/c_i$, $b_i, c_i \in R$, $c_i \neq 0$. Положим $\beta = c_0 \cdots c_n$ и $a_i' = b_i \beta / c_i \in R$. Тогда $f = \frac{1}{\beta} \sum a_i' t^i$. Положим $\alpha = (a_0, \ldots, a_n)$ и $a_i^* = a_i'/\alpha$. Тогда $f = \frac{\alpha}{\beta} \sum a_i^* t^i$. □

Лемма (лемма Гаусса). *Пусть $f, g \in R[t]$ – примитивные многочлены. Тогда fg – примитивный многочлен.*

Доказательство. Запишем

$$f = \sum a_i t^i, \quad g = \sum b_j t^j, \quad fg = \sum c_k t^k,$$

где

$$c_k = \sum_{i+j=k} a_i b_j.$$

Предположим противное. Тогда существует неразложимый элемент $p \in R$ такой, что

$$p \mid c_k, \quad \forall k.$$

По нашему предположению

$$\exists i \quad p \nmid a_i, \qquad \exists j \quad p \nmid b_j.$$

Выберем эти i и j минимальными. Тогда p делит все члены суммы $c_k = \sum_{i+j=k} a_i b_j$ кроме $a_i b_j$. Противоречие. □

Следствие. *Пусть $f, g \in R[t]$, причем g – примитивный многочлен. Если $g \mid f$ в кольце $F[t]$, то $g \mid f$ в кольце $R[t]$. Тогда fg – примитивный многочлен.*

Доказательство. Пусть $f = gh$, где $h \in F[t]$. Имеет место представление $h = \frac{\alpha}{\beta} h^*$, где $\alpha/\beta \in F$ – несократимая дробь и $h^* \in R[t]$ – примитивный многочлен. Тогда $\beta f = \alpha g h^*$. Это противоречит лемме Гаусса. □

Следствие. *Пусть $f \in R[t]$ – примитивный многочлен. Тогда f – неразложимый элемент в кольце $R[t] \iff f$ неприводим в кольце $F[t]$.*

Таким образом неразложимые элементы $f \in R[t]$ бывают двух типов:

- $\deg f = 0$, $f \in R$ – неразложимый элемент,
- $\deg f > 0$, f – примитивный неприводимый в $F[t]$ многочлен.

Лемма. *Пусть $p \in R[t]$ – неразложимый элемент в кольце $R[t]$ и пусть $p \mid fg$, $f, g \in R[t] \Longrightarrow p \mid f$ или $p \mid g$.*

Доказательство. • *Случай* $\deg p = 0$. Запишем $f = af^*$, $g = bg^*$, где $f^*, g^* \in R[t]$ – примитивные многочлены, а $a, b \in R$. По лемме Гаусса f^*g^* примитивный многочлен. Поэтому $p \mid ab \Longrightarrow p \mid a$ или $p \mid b$.

• *Случай* $\deg p > 0$. Тогда p – примитивный многочлен. Пусть $p \nmid f$ в кольце $R[t]$. Тогда $p \nmid f$ в кольце $F[t]$. По соответствующей лемме для многочленов над полем имеем $p \mid g$ в кольце $F[t]$. По следствию $p \mid g$ в кольце $R[t]$. □

Доказательство теоремы. Существование. Запишем $f = af^*$, где $f^* \in R[t]$ – примитивный многочлен, а $a \in R$. Индукцией по степени f^* допускает разложение в произведение

неприводимых примитивных многочленов $\in R[t]$. Поскольку R факториально, то a допускает разложение в произведение неразложимых элементов.

Единственность. Пусть $f = p_1^{m_1} \cdots p_r^{m_r}$ – разложение в произведение неразложимых с наименьшим $\sum m_i$. Индукция по $\sum m_i$. Предположим, что

$$f = p_1^{m_1} \cdots p_r^{m_r} = p_1'^{k_1} \cdots p_s'^{k_s}$$

По лемме $p_1 \mid p_j'$ для некоторого j. Отсюда элементы p_1 и p_j' ассоциированы. Сокращая, получим два разложения f/p_1 с меньшим значением $\sum m_i$. По предположению индукции они совпадают. $\square$