Многочлены над полем рациональных чисел и кольцом целых чисел. Примитивные многочлены и их свойства.

Теорема о разложимости над Q

Пусть $f(x) \in \mathbb{Z}[x]$. $f(x)$ разложим над $\mathbb{Z}$ тогда и только тогда, когда он разложим над $\mathbb{Q}$.

Доказательство

От противного. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ f(x) \in \mathbb{Z}[x]$ разложим над Q, то есть $f(x) = g(x)h(x) \in \mathbb{Q}[x]$. Тогда $g(x) = \dfrac{c_1}{b_1} g_1(x)$ и $h\,(x) = \dfrac{c_2}{b_2} h_1(x)$. При этом $g_1(x)$ и $h_1(x)$ - примитивные. Тогда $f(x) = a_n x^n + \cdots + a_1 x + a_0 = g(x)h(x) = \dfrac{c_1 c_2}{b_1 b_2} g_1(x)h_1(x)$. По лемме Гаусса $g_1(x)h_1(x)$ - примитивный. Если $\dfrac{c_1}{c_2} = \dfrac{p}{q}$, то это означает, что $\dfrac{p}{q} f_1(x)$ - многочлен, то при $q \neq 1$ хотя бы один из коэффициентов которого - рациональная дробь.

Примитивные многочлены

Многочлен $f(x) \in \mathbb{Z}[x]$ называется примитивным, если НОД его коэффициентов равен 1.

Лемма Гаусса

Произведение примитивных многочленов $g(x) \cdot h(x) = f(x)$ является примитивным.

Доказательство

$g(x) = b_k x^k + \cdots + b_1 x + b_0$. При этом НОД$(b_k, \ldots, b_0) = 1$ и $h(x) = c_k x^k + \cdots + c_1 x + c_0$, НОД$(c_k, \ldots, c_0) = 1$. $f(x) = g(x) \cdot h(x)$, то есть $a_n = c_m b_{n-m},\ a_{n-1} = c_{m-1} b_m + c_{m-1} b_{n-m}$, $a_i = c_0 b_i + c_1 b_{i-1} + \cdots + c_i b_{k-i}$. Пусть $f(x)$ - не примитивный. Тогда $\exists d \neq 1$ такое, что d делит любой коэффициент $f(x)$. Будем считать, что d - простое. Возьмём наименьший индекс i_0 такой, что c_{i_0} не делится на d (если все коэффициенты $h(x)$ делятся на d, то $h(x)$ - не примитивный). По аналогии возьмём j_0 такой,что b_{j_0} не делится на d. Рассмотрим коэффициент $a_{i_0+j_0}$ при степени $x^{i_0+j_0}$.

$$a_{i_0+j_0} = c_0 b_{i_0+j_0} + c_1 b_{i_0-1} + \cdots + c_{i_0} b_{j_0} + c_{i_0+1} b_{j_0-1} + \cdots + c_{i_0+j_0} b_0$$

. Тогда $c_{i_0} b_{j_0}$ не делится на d, то есть пришли к противоречию.