т.е. $M(x)$ делится на $m(x)$.

Замечание (о НОД и НОК произвольного набора мн-в)

Д/ отыскания НОД и НОК нескольких (≥ 3) многочленов используют следующие рекуррентные правила:

$$НОД(f_1(x), .., f_{m-1}(x), f_m(x)) =$$
$$= НОД(f_m(x), НОД(f_1(x), ..., f_{m-1}(x)))$$
$$НОК(f_1(x), ..., f_{m-1}(x), f_m(x)) =$$
$$= НОК(НОК(f_1(x), .., f_{m-1}(x)), f_m(x))$$

Кроме того для $НОД(f_1(x), ..., f_m(x)) = d(x)$ справедливо утверждение о линейном представлении:

Существуют такие $u_1(x), .., u_m(x)$, что

$$d(x) = f_1(x)u_1(x) + .. + f_m(x)u_m(x)$$

п 4 Теорема о факторизации

Опр Многочлен $P(x) \in F[x]$, $\deg P(x) > 0$ над неприводимым (точнее, неприводимым над полем F), если $P(x)$ нельзя представить в виде

$$P(x) = P_1(x)\,P_2(x)$$

где $\deg P_i(x) > 0$ $(i = 1, 2)$
$P_1(x), P_2(x) \in F[x]$.

Примеры:

1. $P(x) = ax + b \in F[x]$ неприводим над любым полем F $(a \neq 0)$.
2. $P(x) = x^2 + 1$ неприводим над $\mathbb{Q}$ и $\mathbb{R}$; над $\mathbb{C}$ этот многочлен приводим:

$$x^2 + 1 = (x + i)(x - i)$$

Замечание

Понятие неприводимости многочлена не явл. абсолютным, т.е. если $P(x) \in F[x]$ неприводим и $F \subset \tilde{F}$, то $P(x)$ может оказаться приводимым над $\tilde{F}$

Лемма (основное свойство неприводимых многочленов)

Пусть $p(x), f_1(x), \dots, f_m(x) \in F[x]$, причем $p(x)$ неприводим

Если $f_1(x) \cdot \dots \cdot f_m(x)$ делится на $p(x)$, то один из множителей $f_i(x)$ $(i = 1, \dots, m)$ делится на $p(x)$.

Доказательство

Пусть, от противного, ни один из $f_i(x)$ не делится на $p(x)$.

Тогда

$$НОД(p(x), f_i(x)) = 1$$

для всех $i = 1, \dots, m$

Но в таком случае произведение $f_1(x) \dots f_m(x)$ взаимно просто с $p(x)$ на св-ву взаимно простых многочленов и потому не может делиться на $p(x)$ — противоречие

Теорема 9 (теорема о факторизации)

Пусть $f(x) \in F[x]$, $\deg f(x) > 0$

Тогда существует разложение

$$f(x) = p_1(x) \cdot \dots \cdot p_m(x) \quad (*)$$

где $p_i(x) \in F[x]$ $(i = 1, \dots, m)$ — неприводимый над F мн-н

Если

$$f(x) = q_1(x) \cdot \dots \cdot q_t(x)$$

другое такое разложение, то $t = m$ и, возможно после перенумерации, $p_i(x)$ ассоциирован с $q_i(x)$ $(i = 1, \dots, m)$, т.е. $q_i(x) = c_i p_i(x)$, $c_i \in F$, $c_i \neq 0$

Доказательство

Существование разложения $(*)$ очевидно — достаточно рассмотреть самое длинное разложение многочлена $f(x)$ в произведение нескольких многочленов положительной степени, к-рое обязано состоять из неприводимых многочленов.

Единственность разложения необходимо доказывать, оно неочевидно. Рассм. пример мультипликативной системы, принадлежащий Гильберту.

$$S = \{4k+1 \mid k = 0, \dots\}$$

S – мультипликативное мн-во, содержащее единицу (аналог натурального ряда)

Число $p \in S$ назовем простым, если невозможно представление

$$p = p_1 p_2$$

где $p_1, p_2 \in S$, $p_1 > 1$, $p_2 > 1$

Числа $5, 9, 13, 17, \dots$ – простые. Очевидно, что любое число $a \in S$ разлагается в произведение простых

$$a = p_1 p_2 \cdots p_s$$

Но единственности разложения нет. Например,

$$441 = 49 \cdot 9 = 21 \cdot 21$$

Докажем единственность многочлена $f(x)$ в произведение неприводимых множителей.

Пусть

$$f(x) = p_1(x) p_2(x) \cdots p_s(x) = q_1(x) q_2(x) \cdots q_t(x)$$

два таких разложения. Левая часть этого рав-ва (а значит и правая) делится на $p_1(x)$. Но делится один из многочленов $q_i(x)$ делится на $p_1(x)$.

Пусть, например, $q_1(x)$ делится на $p_1(x)$. Так как $q_1(x)$ неприводимый мн-к, то $q_1(x)$ пропорционален $p_1(x)$, т.е.

$$q_1(x) = c_1 p_1(x)$$

где $c_1 \neq 0$ – константа.

Сокращая на $p_1(x)$ получим:

$$p_2(x) \cdots p_s(x) = c_1 q_2(x) \cdots q_t(x)$$

Применяя это рассуждение нужное кол-во раз, придем к следующему:

$1 = c_1 \cdot \ldots \cdot c_s \, q_{s+1}(x) \cdot \ldots \cdot q_t(x)$

(считаем, что $t \geq s$).

При $t > s$ будем иметь противоречие. Значит, $t \leq s$ и $q_i(x) = c_i p_i(x)$ $(i = 1, \ldots, s)$

Обычно разложение данного многочлена $f(x) \in F[x]$ на неприводимые множители записывают в виде:

$$f(x) = c \cdot p_1(x)^{k_1} \cdot \ldots \cdot p_s(x)^{k_s}$$

где $p_1(x), \ldots, p_s(x)$ попарно непропорциональные нормированные неприводимые над F мн-ки (нормированные — старший коэф. — единица)

Эта запись единственна с точностью до нумерации мн-нов $p_1(x), \ldots, p_s(x)$

Указанная запись наз. КАНОНИЧЕСКИМ РАЗЛОЖЕНИЕМ мн-на $f(x) \in F[x]$.

Если известно каноническое разложение мн-нов $f_1(x), \ldots, f_m(x) \in F[x]$, то НОД и НОК этих мн-в могут быть найдены при помощи хорошо известного типового правила

Замечание

На практике предпочтительнее, вообще говоря, использовать для отыскания НОД и НОК алгоритм Евклида.

Опр Пусть $f(x) \in F[x]$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$

Производной этого мн-на наз. многочлен вида

$$f'(x) = n a_n x^{n-1} + \ldots + a_1 \in F[x]$$

Здесь $k a_k$ понимается как $\underbrace{a_k + \ldots + a_k}_{k \text{ слагаемых}}$

Пример

$F = F_2$ — поле из 2х эл-тов

Пусть $f(x) = x^2 + 1$. Тогда $f'(x) = (1+1)x = 0$

(*) Далее будем считать, что F — поле нулевой характеристики ($\mathrm{char}\, F = 0$), т.е. суммы вида $1 + 1 + \ldots + 1$ отличны от нуля. В этом случае, как легко видеть

$$\deg f'(x) = \deg f(x) - 1$$